CALIFORNIA HIGH-SPEED TRAIN SYSTEM

CHSTS SAFETY AND SECURITY MANAGEMENT PLAN

Revision 0.2

Prepared by:	-- Original signature on file -- John Cockle, PMT Safety Specialist	02/14/2013 Date
Reviewed by:	-- Original signature on file -- John Sheehan, PMT Safety Manager	02/15/2013 Date
Approved by:	-- Original signature on file -- Joseph Metzler, PMT Operations Manager	02/15/2013 Date
Reviewed by:	-- Original signature on file -- Michael Lewis, PMO	02/26/2013 Date
Released by:	-- Original signature on file -- Brent Felker, PMT Program Director	04/29/2013 Date

Document	Sections/Pages Affected	Date of Document
Rev 0.0	Initial Draft	06/30/11
Rev 0.1	2ND Draft	01/06/2012
Rev 0.2	3rd Draft – FRA Comments, Security Update, S/S Policy, Committee charters, changes in Authority structure	02/14/2013

TABLE OF CONTENTS

FIGURES

TABLES

APPENDICES

ACRONYMS AND ABBREVIATIONS

Acronym or Abbreviation	Definition
Authority	California High-Speed Rail Authority
CEHL	Certifiable Elements and Hazards Log
CFR	Code of Federal Regulations
CHST	California High-Speed Train
CHSTS	California High-Speed Train System
CIL	Critical Items List
CPUC	California Public Utilities Commission
DHS	Department of Homeland Security
EMT	Engineering Management Team
FD	Final Design Phase
FLSSC	Fire/Life Safety and Security Committee
FMEA	Failure Mode Effects Analysis
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
FTAn	Fault Tree Analysis
ICS	Initial Construction Segment
OHA	Operating Hazard Analysis
OMT	Operations and Maintenance Team
PE	Preliminary Engineering Phase
PHA	Preliminary Hazard Analysis
PMO	Program Management Oversight
PMP	Project Management Plan
PMT	Program Management Team
PTEPP	Passenger Train Emergency Preparedness Plan
QC	Quality Control
RAC	Rail Activation Committee
RAP	Rail Activation Plan
RC	Regional Consultant

SITC	System Integration Testing Committee
SSCP	Safety and Security Certification Plan
SSEC	Safety and Security Executive Committee
SHEA	Software Hazard Effects Analysis
SiSHA	Site-Specific Hazard Analysis
SSHASP	Site-Specific Health and Safety Plan
SSI	Sensitive Security Information
SSMP	Safety and Security Management Plan
SSPC	Safety and Security Program Committee
SSSP	Site-Specific Security Plan
TSA	Transportation Security Administration
TVA	Threat and Vulnerability Assessment
V&V	Verification and Validation

REFERENCE DOCUMENTS

The following documents are referenced in this SSMP:

- 49 CFR Parts 200-299, Federal Railroad Administration regulations
- 49 CFR Part 633, Federal Transit Administration *Project Management Oversight*
- 49 CFR Part 659, Federal Transit Administration *State Safety Oversight*
- ANZI Z590.3-2011 *Prevention through Design*, 01/23/2012
- California Code of Regulations Title 8 Construction Safety Orders
- Department of Defense Military Standard 882E *System Safety*, 5/11/2012
- FTA *Handbook for Transit Safety and Security Certification*, 11/2002
- FTA document *Hazard Analysis Guidelines for Transit Projects*, 01/2000.
- FTA document *Public Transportation System Security and Emergency Preparedness Planning Guide*, 01/2003.
- FTA Circular 5800.1 *Safety and Security Management Guidance for Major Capital Projects*, dated 8/1/07
- ISO 31000 Risk Management Standard

1.0 MANAGEMENT COMMITMENT AND PHILOSOPHY

1.1 Safety and Security Policy Statement

Safety and Security Policy Statement

It is the policy of the California High-Speed Rail Authority (Authority) to perform work on the California High-Speed Train System (CHSTS) in a manner that ensures the safety and security of passengers, employees, contractors, emergency responders, and the public. The application of system safety and security comprises a fundamental hazard and vulnerability management process that incorporates the characteristics of planning, design, construction, testing, operational readiness, and subsequent operation of the high-speed rail system. Safety and security are priority considerations in the planning and execution of all work activities on the CHSTS.

All trains, facilities, systems and operational processes must be designed, constructed, and implemented in a manner that promotes the safety and security of persons and property. The design, construction, testing, and start-up of the CHSTS will comply with applicable safety and security laws, regulations, requirements and railroad industry practices. The Authority will maintain or improve upon the public transit and railroad industry standards for safety and security. Through the Reliability, Availability, Maintainability, and Safety (RAMS) Program a standard of safety will be established that is as safe as or safer than conventional U.S. railroad operations and in conformance with the best practices and standards for safety in the international high-speed rail industry. The design, construction, testing, and start-up of the CHSTS will be accomplished in compliance with this standard.

The Authority is committed to providing a safe and secure travel and work environment. Therefore, safety, accident prevention, and security breach prevention must be incorporated into the performance of every employee task. All Authority, Program Management Team, and contractor personnel, subcontractors and employees are charged with the responsibility for ensuring the safety and security of passengers, employees, contractors, emergency responders, and the public who come in contact with the CHSTS. Each individual and organization is responsible for hazard and vulnerability management, for applying the processes that are designed to ensure safety and security, and for maintaining established safety and security standards, consistent with their position and organizational function. Through a cooperative team effort and the systemic application of safety and security principles, the CHSTS will be designed, constructed, tested, and placed into service in a safe and secure manner.

Jeff Morales — 12·5·12

Jeffrey Morales, CEO
California High-Speed Rail Authority

Date

1.2 Background

The Federal Railroad Administration (FRA) requires that the Authority implement safety and security principles and processes throughout the development and operation of the California High-Speed Train System (CHSTS). Absent federal regulations that govern the completion of major capital projects, the Federal Railroad Administration looks to the Federal Transit Administration (FTA) regulations for guidance. Federal Transit Administration (FTA) regulations found at 49 CFR 633 requires the development of a *Project Management Plan* (PMP) for every major capital transit project. As described in FTA Circular 5800.1 *Safety and Security Management Guidance for Major Capital Projects*, (dated 8/1/07) a *Safety and Security Management Plan* (SSMP) is the element of the PMP that manages project safety and security activities, responsibilities, and verification processes throughout the project life cycle.

This document fulfills the FRA requirement for managing safety and security in the development and operation of the CHSTS.

The SSMP does not carry over into revenue operations, but will lead to development of a System Safety Program Plan and Security and Emergency Preparedness Plan to govern safety and security for the operating system prior to the start of revenue service. The FRA is in the process of promulgating regulations that require the application of a System Safety Program Plan to inter-city passenger railroad operations.

1.3 Purpose of the SSMP

The SSMP formalizes the technical and management strategies for determining safety and security risk acceptance throughout the CHSTS life cycle, from the design phase through the start of revenue service and is applied to each segment undertaken in turn. The SSMP defines the process for identifying, evaluating, and resolving safety hazards and security vulnerabilities associated with future railroad operations of the System prior to the start of revenue service. This process helps to ensure the achievement of the highest practical level of operational safety and security for the riding public, the employees, and anyone coming into contact with the CHSTS.

The purpose of the SSMP is to define the safety and security activities of the CHSTS and methods for identifying, evaluating, and resolving potential safety hazards and security vulnerabilities. It establishes responsibility and accountability for safety and security during the preliminary engineering, final design, construction, testing, and start-up phases of CHSTS development. Specifically, the SSMP does the following:

- Establishes the Authority‘s commitment and philosophy to achieve the highest practical level of safety and security for the Authority’s staff, Program Management Team (PMT) staff, contractors, emergency responders, and members of the public that come into contact with the CHSTS
- Establishes and manages safety and security activities intended to minimize risk of injury and property damage, and to maximize the safety and security for the CHSTS passengers, employees, and the public
- Integrates the safety and security functions and activities throughout the CHSTS and its organizational structure
- Defines the safety and security responsibilities between the Authority and CHSTS design, construction, and start-up teams
- Defines the process for the documentation and verification of safety and security activities
- Evaluates project phases and activities to ensure continued development and advancement of safety and security principles
- Establishes the framework for construction safety and security

1.4 Applicability and Scope of SSMP

The SSMP is applicable to all phases of CHSTS development, from preliminary engineering through final design, construction, testing and the start of revenue service. The SSMP encompasses all equipment, infrastructure, operating and maintenance plans and procedures associated with the CHSTS.

1.4.1 Project Description

The California High-Speed Train System will construct a state-of-the-art, statewide, high-speed performance passenger railroad based on operating practices and designs of existing high-speed rail networks in Europe and Asia which have had extraordinary performance and safety records. The CHSTS will require certification by federal and other regulatory agencies which have indicated they are open to approaches which provide equivalent or better safety than existing rail regulations in the United States.

The Authority's eventual goal is to develop a system of more than 800 route miles that provides high-speed rail service between the major metropolitan centers of the San Francisco Bay Area and Sacramento in the north, through the Central Valley, to Los Angeles, Anaheim, Irvine and San Diego in the south.

The CHST trains will operate at speeds up to 220 mph within its dedicated or shared-use corridors where the CHSTS has sole use of a track, and up to 125 mph in shared-use conditions where there is joint use of tracks with other passenger trains. There will be no joint use of tracks with freight trains on shared-use tracks. Freight operations, where applicable, will be temporally separated. No hazardous materials will be transported or permitted to be transported by others on Authority dedicated tracks.

The service will use high-speed steel-wheel on steel-rail technology which has been service-proven in Asia and Europe and provides a high level of service in terms of safety, comfort, and reliability. The system will operate on a mostly dedicated, fully grade-separated standard gage track with electric trains powered through the use of an overhead contact system. The right-of-way will make use of tunneling and elevated structures to achieve an ideal alignment and profile. Automotive, animal, other railroad and non-railroad equipment crossings will be accomplished by means of an underpass or overpass.

The system will include an Automatic Train Control (ATC) system based on designs for similar high-speed environments in Europe and Asia, modified only where necessary to meet regulatory requirements and functional and performance needs specific to the CHSTS. The ATC system will cover all functions of a train control system including both safety critical and non-safety critical operations and will incorporate Positive Train Control in compliance with FRA regulations. A hazard detection system will be applied throughout the CHSTS where supported by hazard analysis to alert the operating control center of natural events such as seismic activity, excessive wind speeds, high water levels, and excessive ambient temperature levels that trigger a system response; and other events such as vehicle or rail car intrusion, and trespassers.

1.4.2 Phased Implementation

Although Preliminary Engineering Phase activities will occur simultaneously for the entire system, the Final Design and Construction Phase activities will be developed in phases according to geographic segments, due to the size of the eventual system. The Initial Construction Segment (ICS) has been designated as a point north of Madera to a point north of Bakersfield. Subsequent segments will extend north and south from the ICS.

The Initial Operating Segment (IOS) will encompass several construction segments, with high-speed operations planned between Merced in the north and Palmdale in the south. The IOS will eventually be expanded into what is termed "Bay to Basin", providing high-speed rail service from the greater San Francisco Bay Area to the greater Los Angeles Basin. The SSMP has been developed with processes that will ensure conformance to system safety goals and requirements throughout the life-cycle of the CHSTS and while various segments are under different development phases simultaneously.

1.4.3 SSMP Scope

This SSMP encompasses the following equipment, facilities, plans, and procedures as they relate to the System.

- System-Wide Elements − includes the passenger vehicles, train control and signaling, voice and data communications, closed-circuit television cameras and recorders, overhead contact system, traction power substations, track, and auxiliary vehicles and equipment
- Fixed Facilities − includes rail stations; pedestrian overpasses and underpasses; highway overpasses and underpasses; aerial and other elevated structures; below-grade structures and tunnels; operations and maintenance facilities including storage yards, shops, and sidings; administrative facilities; and the Central and Regional Control Facilities.

- Safety and Security Plans and Procedures − includes items such as Safety and Security Certification Plan (SSCP), Safety and Security related Design Criteria, Passenger Train Emergency Preparedness Plan (PTEPP), System Safety Program Plan, and Security and Emergency Preparedness Plan.
- Procedures and Instructions − includes items such as: Operations and Maintenance procedures, rulebooks and manuals; and training programs for operating, maintenance and management employees, employee qualifications, contractor training, and emergency responder training.

1.5 SSMP Goals and Objectives

1.5.1 Goals

The goals of the SSMP are as follows:

- Ensure that the system initiated into revenue service is safe and secure for passengers, employees, emergency response personnel, and the general public through a formal program of safety and security certification
- Ensure that the design, acquisition, construction, fabrication, installation, and testing of critical elements of CHSTS development will be verified for conformance with the established safety and security requirements and validated for achieving an effective level of safety and security
- Ensure that a mechanism is in place for the resolution of any restriction to full safety and security certification
- Establish a Construction Safety and Security Program that provides appropriate safeguards against injuries to employees and the public, damage to property and the environment, as well as minimizes security breaches, during all CHSTS work activities
- Achieve a level of risk that is acceptable to the Authority through a systematic approach to hazard and threat/vulnerabilities management

1.5.2 Objectives

The SSMP goals will be achieved by meeting the following objectives:

- Identifying, evaluating, resolving, and documenting safety hazards and security vulnerabilities at the earliest possible phase of CHSTS development, applying the Prevention through Design principle where possible
- Establishing specific safety and security requirements for the CHSTS based on applicable safety and security regulations, codes, standards, guidelines, and recognized best practices both domestically and internationally where applicable
- Verifying that all final drawings, specifications, and contracts issued for the CHSTS conform to the established safety and security requirements
- Implementing CHSTS construction safety and security programs in conformance with established construction safety and security requirements and complying with the California Occupational Safety and Health Administrative safety regulations for construction projects
- Verifying all CHSTS facilities, systems, and equipment have been designed, built, procured, installed, inspected, and tested in accordance with the design criteria and specifications
- Establishing and documenting the qualifications and training programs for all personnel who will operate and maintain the CHSTS in revenue service
- Verifying completion of training of personnel who will respond to emergencies, including CHSTS personnel and emergency responders, on the CHSTS emergency procedures, equipment, and operations
- Conducting and documenting emergency exercises and drills prior to the start of revenue service

- Documenting safety, security, and emergency rules and procedures for CHSTS employees, staff, and contractors in the form of rulebooks, standard operating procedures, emergency operating procedures, and other documents
- Maintaining a process to manage and track open safety and security issues resulting from design deviations, change orders, and non-conformances from inception through closure and acceptance
- Documenting final Safety and Security Certification for the CHSTS segment under consideration by means of a Final Safety and Security Certification Verification Report prior to placing that segment into revenue service
- Ensuring coordination with the Federal Railroad Administration, California Public Utilities Commission, the Transportation Security Administration, the Office of the State Fire Marshal, and other external agencies as applicable

1.6 SSMP Review and Updates

The SSMP will be reviewed at least annually, whenever the Program Management Plan or other reference documents are modified, and following any SSMP audit to ensure the safety and security management program remains current and applicable. If revised, the SSMP will be re-issued to all SSMP recipients. The SSMP will be updated to reflect changes in the CHSTS, the Authority's organizational makeup, or the safety and security management program requirements. The review and update process will be the responsibility of the Authority with the oversight and coordination of the Authority's System Safety Manager.

The Federal Railroad Administration is developing regulations for inter-city passenger rail system safety programs, to be codified under 49 CFR, Part 270. This SSMP is written to be in conformance with proposed regulations for 49 CFR, Part 270 and will be transformed into a System Safety Program Plan when the regulations are finalized.

1.7 SSMP Applicability to Third Parties

The safety and security requirements for third party assets (adjacent infrastructure or operations, shared-use corridors, utility interfaces, etc.) will be developed following the safety and security management program of the applicable third party but in conformance to the processes and requirements of this SSMP. Safety and security certification of third party elements shall conform to the Safety and Security Certification Program requirements of the third party and Section 7.0 of this SSMP.

2.0 INTEGRATION OF SAFETY AND SECURITY INTO THE CHSTS DEVELOPMENT PROCESS

2.1 Safety and Security Activities

This section describes the safety and security activities that have been or will be performed during the major phases of the project. A list of the basic activities and the desired milestone goals are presented in

Table 2-1. The California High-Speed Train System has four phases:

- Preliminary Engineering
- Final Design
- Construction
- Testing and Startup of Revenue Operations

Although Preliminary Engineering Phase activities will occur simultaneously for the entire system, the Final Design and Construction Phase activities will be developed in phases according to geographic segments, due to the size of the eventual system. The SSMP has been developed with processes that will ensure conformance to system safety goals and requirements throughout the life-cycle of the CHSTS and while various segments are under different development phases simultaneously.

Within each phase of the CHSTS, activities are identified to determine the safety- and security-related certification activities expected to be accomplished at each project milestone. The California High-Speed Rail Authority will apply a detailed and thorough safety and security certification program. The safety and security certification program, as described in Section 7.0 of this SSMP, will ensure that the project achieves all safety and security requirements in design criteria and specifications and that the safety and security contents of the plans, procedures, and training materials are systematically reviewed and revised as required.

Leading up to and through the Preliminary Engineering phase of the project, the safety and security activities encompass the following:

- Develop the SSMP, including a process for achieving safety and security certification, to meet all Federal Railroad Administration (FRA) requirements for a safety and security management plan in a major capital project, in conformance with the Federal Transit Administration's Circular 5800.1 *Safety and Security Management guidance for Major Capital Projects*.
- Develop a list of safety-critical and security-critical elements and items for the CHSTS Preliminary Hazard Analyses.
- Specify safety and security certification requirements, in conformance with the *CHSTS Verification and Validation Management Plan*, in contract documents. Safety and security certification requirements will be part of the scope of work for the design/build contractors during the Final Design and Construction phases of the project.
- Implement a hazard and certification tracking system.
- Perform Preliminary Hazard Analysis (PHA) and a Threat and Vulnerability Assessment (TVA) to identify certifiable elements and hazards/vulnerabilities requiring mitigation. Identify hazard/vulnerability mitigation from the PHA and TVA to be incorporated into preliminary and final designs. Perform additional analysis as required.
- Develop design criteria conformance checklists. The tracking system will be an integrated subset of the Verification & Validation program applied throughout the CHSTS.

Table 2-1 Project Safety and Security Activities Matrix

Task No.	Safety and Security Task	Project Phase			
		Prelim. Engr.	Final Design	Construction	Testing and Startup
1	Develop Safety and Security Management Plan (SSMP)	√	⇒	⇒	⇒
2	Identify Certifiable Elements and Items	√	⇒	⇒	⇒
3	Specify Safety and Security Certification Requirements into Contract Documents	√	⇒		
4	Implement Certification Tracking System	√	⇒	⇒	⇒
5	Conduct Preliminary Hazard Analysis (PHA) and Threat and Vulnerability Assessment (TVA) and Resolve Unacceptable Hazards and Vulnerabilities	√	⇒	⇒	⇒
6	Develop Design Criteria Conformance Checklists	√	⇒		
7	Conduct Independent Safety and Security Audits		√	⇒	⇒
8	Verify Design Criteria Conformance Checklists and Issue Certificates		√	⇒	
9	Develop Construction Specification Conformance Checklists		√	⇒	
10	Develop Safety-Related Testing Conformance Checklists			√	⇒
11	Verify Specification Conformance Checklists			√	⇒
12	Verify Safety-Related Testing Conformance Checklists				√
13	Verify Operations and Maintenance Manuals Conformance			√	⇒
14	Complete Contractor Training			√	⇒
15	Complete Rules and Procedures and Issue Certificates			√	⇒
16	Complete Operations Training and Issue Certificates				√
17	Complete Emergency Services Training				√
18	Complete Emergency Response Exercises				√
19	Issue Final Safety/Security Certificate of Conformance				√
20	Issue Final Safety/Security Certification Verification Report				√

Note: √ = Task activity initiated
⇒ = Task activity updated

2.2 Procedures and Resources

2.2.1 Procedures

A *CHSTS Project Management Plan* (PMP) for the system has been prepared. The PMP establishes the framework for managing and administering all activities related to implementation of the system and provides guidance for the coordination of activities. The PMP identifies that the PMT is responsible for developing the basic design requirements of the high-speed rail system, ensuring that common approaches for the environmental and outreach work are used through the entire alignment, preparing and helping execute bid and procurement processes for design, construction, maintenance, and operations, and managing the work of or coordinating with a variety of other consultants to the Authority, notably the Regional Consultants (RC).

A major component of the PMP is this *Safety and Security Management Plan*, describing processes for identifying and managing hazards and vulnerabilities associated with the CHSTS. It is the responsibility of the Authority to ensure that the management of identified safety hazards and security threats and vulnerabilities is effective and integrated throughout the design, construction, testing, and startup phases of the CHSTS.

The verification and validation process will be applied throughout the CHSTS for the purpose of tracking and verifying that critical elements are incorporated into all project phases. Critical elements include safety-critical and security-critical elements as identified though the hazard management processes identified in this SSMP.

2.2.2 Resources

The Chief Executive Officer authorizes the SSMP, ensuring that it is applied throughout the CHSTS. The Risk Manager administers and oversees the SSMP. The Authority will provide additional safety and security management resources for executing the system safety and security activities during the Preliminary Engineering phase. Further resources and responsibilities will be identified as the system progresses into later phases, culminating in startup and commissioning.

The budget and schedule for implementation of the SSMP is revised each year and is held with the Risk Manager. This assures that the requirements of the SSMP are executed by the Authority, supported by the PMT, during the Preliminary Engineering phase and in subsequent phases of the project. This includes, but is not limited to, the performance of safety analyses and security assessments at the appropriate phases of the project; implementation of a Safety and Security Certification Program beginning at Preliminary Engineering and continuing through each subsequent phase of the project; and a process to ensure that safety issues and security concerns are addressed and tracked to resolution.

2.3 Interfacing with Management

The California High-Speed Rail Authority Chief Executive Officer through the Authority Risk Manager has the ultimate decision-making authority for safety and security issues and is responsible for communication of safety and security issues to the Authority Board of Directors. The Risk Manager will oversee the overall implementation of the safety and security program and will report to the Safety and Security Program Committee the progress and challenges in its implementation. The Safety and Security Program Committee will communicate the safety and security issues to the Authority executive management through reports to the Safety and Security Executive Committee.

Successful implementation of the SSMP will also require significant interaction between various members of the Authority, the Program Management Team, Regional Consultants, Engineering/Construction Managers, and Emergency Response Agencies. These interactions will occur during regularly scheduled meetings of the Safety and Security Program Committee that focus on the safety and security aspects of the system.

3.0 SAFETY AND SECURITY RESPONSIBILITIES

3.1 Roles and Responsibilities

The California High-Speed Rail Authority (Authority) is responsible for developing a high-speed train system in California in a safe and secure manner, ensuring that all trains, facilities, systems and operational processes are designed, constructed, and implemented in a manner that promotes the safety and security of persons and property. The Authority has the ultimate authority and responsibility for the implementation of the *Safety and Security Management Plan* (SSMP) for this system. The Authority is tasked to prepare a plan and design for the system, conduct environmental studies and obtain necessary permits, and undertake the construction and operation of a high-speed train passenger network in California. These tasks are collectively referred to as the California High-Speed Train System.

The Risk Manager administers and oversees the implementation and activities of the Safety and Security Program. The Authority's primary vehicle for oversight of the safety and security activities is a two-tiered organization of safety and security committees (explained in detail in Section 3.3).

The Federal Railroad Administration (FRA) is the lead agency for the Federal Environmental Impact Statement. The FRA is also the primary regulatory agency responsible for approving and certifying the system safety and security aspects of the CHSTS. At the state level, the California Public Utilities Commission has specific responsibilities within the system safety and security program and the electric traction power system that affects the CHSTS.

The Authority has contracted with Parsons Brinckerhoff (PB) as the Program Management Team (PMT), and five Regional Consultant (RC) teams to conduct the preliminary engineering on specific segments of the line and provide overall Program Management for the CHSTS.

The PMT is responsible for the basic design of the high-speed train system, including ensuring that system safety and security is applied consistently and effectively for the entire CHSTS alignment and across all phases of the project.

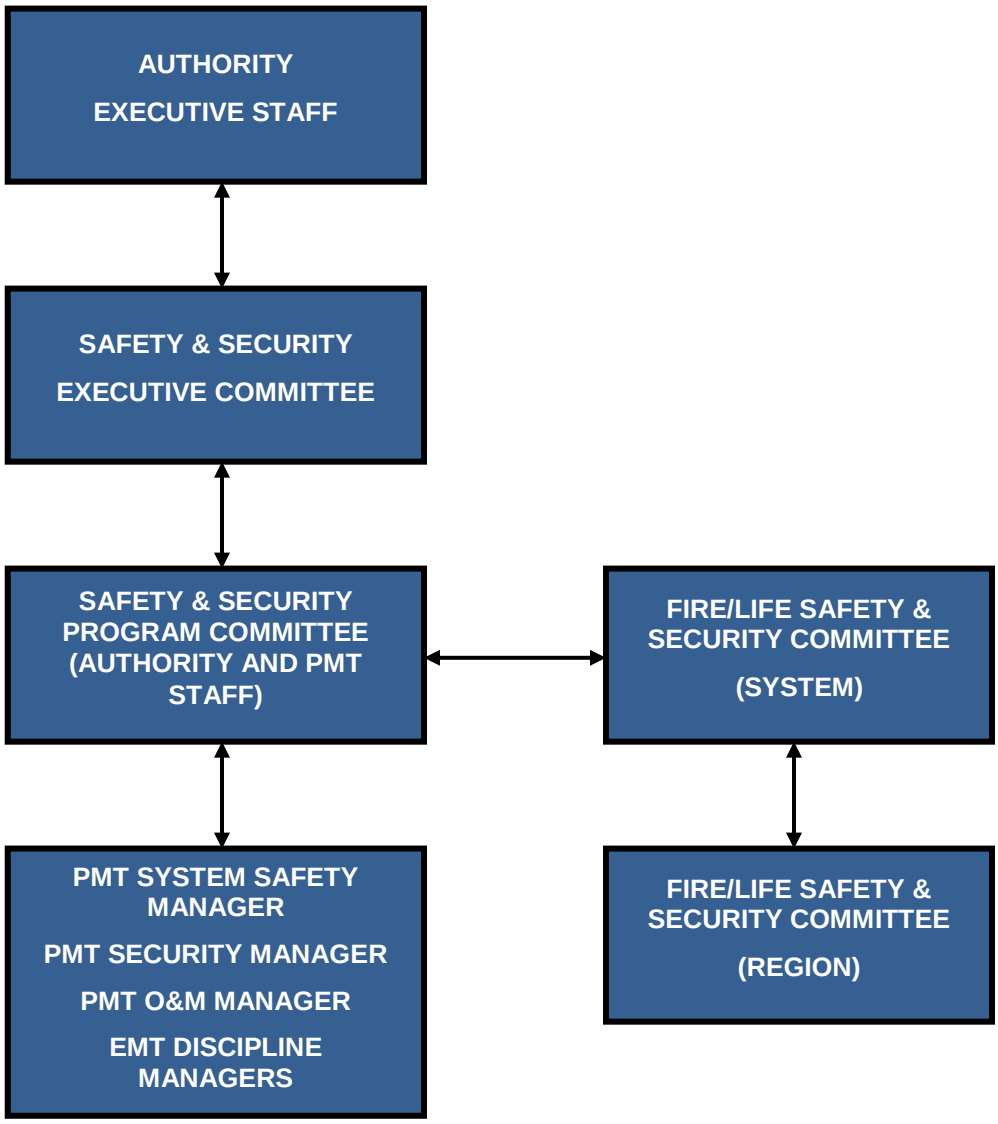
The PMT Safety and Security Managers will support the Authority Risk Manager in the application of safety and security in all aspects and phases of the project with support from the Program Deputy Directors, Discipline Managers, and Regional Managers. This support will ensure that other individual project staff members perform in accordance with the SSMP in establishing and overseeing the safety and security management tasks. The PMT's primary vehicle for input to and support of the safety and security activities is the Safety and Security Program Committee (explained in detail in Section 3.3.2).

Staff members assigned to the CHSTS by the Authority, PMT, contractors, consultants, emergency response agencies, FRA and CPUC are responsible for ensuring that the design, construction, installation, and testing of all safety-critical and security-critical system elements of the system are evaluated for conformance with the safety and security requirements and verified for operational readiness before completing each phase of the project.

Refer to Figure 3-1 for the CHSTS organizational chart for safety and security activities.

The PMT supports as the Authority in the management of safety and security in the development of the CHSTS. This SSMP shall be updated to reflect any significant changes in the organizational structure or definition of responsibilities with respect to safety and security in the CHSTS.

Figure 3-1 CHSTS Organization for Safety and Security Activities



3.2 Authority Organization

The Authority has a nine-member policy board and a core staff, supported by contract with private consulting firms (the Program Management Team, Regional Consultants and other specialty firms) to carry out the project's system safety and security programs, environmental studies, project planning and engineering work under the supervision and guidance of Authority staff. The Authority's Risk Manager is responsible for safety and security activities, reporting directly to the Chief Executive Officer.

The project organization will remain in place throughout the CHSTS development process; however, the composition of the project organization may be revised to respond appropriately to the changing project needs as the project proceeds through from the preliminary engineering phase through to the start of revenue service. The Authority project organization during the initial project phases is composed of Authority and Program Management Team staff supplemented by Regional Consultant staff. In each

phase, the Authority will use the assistance of the PMT to manage project-related activities, as well as further assistance from professional engineering and other project management consulting firms.

The current California High-Speed Rail Authority organization is shown in Appendix A.

3.2.1 Authority Chief Executive Officer

The Authority Chief Executive Officer oversees and directs the management of all Authority staff and the Program Management Team. The day-to-day management of the development activities for the California High-Speed Train System is the functional responsibility of the Authority Program Director under the direction of the Authority Chief Executive Officer. The Authority Chief Executive Officer ensures that Authority resources are allocated to meet the SSMP goals and objectives, and is ultimately responsible for execution of the *Safety and Security Management Plan* through the Authority Risk Manager. The Authority Chief Executive Officer chairs the Safety and Security Executive Committee and reports to the Authority Board of Directors.

3.2.2 Authority Risk Manager

The Authority Risk Manager is responsible for the management of all safety and security activities associated with the development and implementation of the CHSTS. The Authority Risk Manager sits on the Safety and Security Executive Committee, chairs the Safety and Security Program Committee, and advises the Authority on Policy decisions with regard to safety and security. The Authority Risk Manager reports directly to the Authority Chief Executive Officer and coordinates safety activities with the PMT Safety and Security Managers.

The Authority Risk Manager has the authority and responsibility for, but is not limited to the following:

- Ensuring that the SSMP requirements and processes are being implemented and that SSMP goals and objectives are being achieved
- Oversight of the PMT safety and security activities
- Developing corrective action plans (CAPs) that result from accident/incident investigations, hazard analyses, certification of Certifiable Items List (CIL), and safety and security reviews and audits; and tracking corrective actions through closeout to ensure that all identified deficiencies are adequately mitigated or controlled
- Providing oversight for the Contractors' job site safety and programs
- Reviewing and supporting Authority decision for Contractor's safety submittals
- Investigating accidents and incidents on behalf of the Authority
- Reporting unacceptable hazardous conditions to executive management as soon as possible
- Fulfilling the role of Chair of the Safety and Security Program Committee
- Fulfill the role of Chair for the Fire and Life-Safety and Security Statewide and Regional Committees

3.2.3 PMT System Safety Manager

The PMT System Safety Manager will support the Authority in the implementation and completion of all safety activities associated with the development of the CHSTS. The PMT System Safety Manager will coordinate safety activities with the PMT Security Manager, PMT Discipline Managers, and sit on the Safety and Security Program Committee, Safety and Security Executive Committee, and Fire and Life-Safety and Security Committees as requested. The PMT System Safety Manager's role on the Committees is to ensure that safety and security are not compromised by other priorities of the design and construction teams.

The PMT System Safety Manager has the responsibility for, but is not limited to, the following:

- Performing hazard analyses of CHSTS elements and design criteria to determine any potential hazards that may be created by system development, expansion or modification, and supporting the development of mitigating and controlling factors to address such hazards
- Participating in the project design reviews, including overseeing and administering formal safety and security certification programs
- Working with PMT engineering, operations and maintenance staff to ensure that the system is being designed to safety and security criteria
- Fulfilling the role of Secretary for the Safety and Security Program Committee, and the Fire and Life-Safety and Security Statewide and Regional Committees
- Performing other safety-related activities as requested by the Authority

3.2.4 PMT Security Manager

The PMT Security Manager will support the Authority Risk Manager in the implementation and completion of all security activities associated with the development of the CHSTS. The PMT Security Manager will coordinate security activities with the PMT Safety Manager, PMT Discipline Managers, and sit on the Safety and Security Program Committee, Safety and Security Executive Committee, and Fire and Life-Safety and Security Committees as requested. The PMT Security Manager's role on the Committees is to ensure that security requirements are not compromised by other priorities of the design and construction teams.

The PMT Security Manager has the responsibility for, but is not limited to, the following:

- Performing threat assessments of CHSTS operating environments and design criteria to determine any potential vulnerabilities that may be created by system development, expansion or modification, and supporting the development of mitigating and controlling factors to address such vulnerabilities
- Participating in the project design reviews, including overseeing and administering formal safety and security certification programs
- Working with PMT engineering, operations and maintenance staff to ensure that the system is being designed to safety and security criteria

3.2.5 Other Managers

The managers of the following disciplines will be responsible for implementing the SSMP requirements and process in their respective areas, participating in the SSPC and for supporting the Risk Manager as required:

- Engineering, including Infrastructure and Systems;
- Operation and Maintenance;
- Rolling Stock;
- Integration and Regulatory Approvals;
- Project Risk;
- Contracts and Procurement;
- Verification and Validation.

3.3 Committee Structure

Chapter 2 of the PMP describes the function of various project committees. In addition, safety and security committees listed below will be established to facilitate review of issues and to provide a forum for discussion and resolution.

3.3.1 Safety and Security Executive Committee

The Safety and Security Executive Committee (SSEC) and its members will ensure that the CHSTS is designed, built, and implemented in a safe and secure manner. The SSEC will achieve this goal by providing oversight of the application of the SSMP through all phases of the CHSTS development and to act as a conduit to informing and assuring Authority executive management of safety and security issues.

The Safety and Security Executive Committee will address safety and security issues which are Authority policy considerations, require Authority approval, require Authority direction for resolution of a dispute, or constitute final acceptance of safety and security certification.

The duties and responsibilities of the Safety and Security Executive Committee are as follows:

- Approve the initial version of the SSMP and subsequent updates;
- Oversee the application of the SSMP through all CHSTS development phases;
- Authorize the establishment of the Safety and Security Program Committee (SSPC);
- Review and approve regular reports of safety and security activities from the SSPC;
- Resolve safety and security issues that cannot be resolved at the SSPC level;
- Review and approve safety and security certification Certificates of Conformance and a final Certification Verification Report prior to the advancement into the next project phases;
- Provide a forum for safety and security discussions among Authority Executive Management, discipline leads, and PMT Management.

The Safety and Security Executive Committee comprises the following persons:

- Authority Chief Executive Officer (Chairperson);
- Authority Risk Manager
- Authority Regional Directors;
- Authority Chief Operating Officer;
- Authority Chief Engineer;
- Authority Chief Counsel;
- PMT Program Director (advisory role);
- PMT System Safety Manager (Secretary - advisory role);
- PMT System Security Manager (advisory role).

The Chairperson of the SSEC is the Authority Chief Executive Officer or a designated Authority executive management representative. If a designated member of the SSEC is unable to attend a SSEC meeting, they must assign an appropriate representative.

The SSEC Charter, Technical Memorandum 500.02, can be found in Appendix C of this SSMP.

3.3.2 Safety and Security Program Committee

Working at the project delivery level, the Safety and Security Program Committee (SSPC) will ensure that the CHSTS is designed, built, and implemented in a safe and secure manner. The SSPC will achieve this goal by providing oversight of the application of the SSMP through all phases of the CHSTS development and to act as a conduit to informing and assuring Authority executive management (through the SSEC) of safety and security issues affecting the project.

The SSPC will address safety and security issues which are directed to it by the SSEC, require project delivery level resolution, require elevation to the SSEC for Authority direction for resolution, or constitute preliminary review and approval of Safety and Security Certification.

The duties and responsibilities of the Safety and Security Program Committee are as follows:

- Recommend to the SSEC the initial version of the SSMP and subsequent updates;
- Oversee the application of the SSMP through all CHSTS development phases;
- Review and approval of PHAs and TVAs as they are developed or updated;
- Tracking of identified hazards or vulnerabilities listed on Certified Elements and Hazards List using the V&V Requirements Management Tool database;
- Provide regular reports of safety and security activities to the SSEC;
- Forward to the SSEC for resolution any safety and security issues that cannot be resolved at the SSPC level;
- Review and approve safety and security certification Certificates of Conformance and a Final Certification Verification Report;
- Forward Certificates of Conformance and a final Certification Verification Report to SSEC for Authority acceptance prior to the start of applicable testing phases or startup of revenue service;
- Provide a forum for safety and security discussions among PMT staff members and a conduit for safety and security issues to the Authority through the SSEC.

The Safety and Security Project Committee is made up of the following persons:

- Authority Risk Manager (Committee Chairperson);
- Authority Regional Directors;
- PMT System Safety Manager (Committee Secretary);
- PMT System Security Manager;
- PMT Program Director
- PMT O&M Manager;
- EMT Discipline Managers;
- PMT Verification & Validation Manager;
- PMT Contracts Manager;
- PMT Project Risk Manager;
- PMT RAMS Manager.

If a designated member of the SSPC is unable to attend a SSPC meeting, they must assign an appropriate representative.

The SSPC Charter, Technical Memorandum 500.03, can be found in Appendix D of this SSMP.

3.3.3 Fire and Life Safety and Security Committees (FLSSC)

The Fire and Life Safety and Security Committees (FLSSC) will be composed of representatives from fire, police and local building code agencies assigned to two levels of standing committees: a system FLSSC and several regional FLSSC working on a local level. The CHSTS will form the FLSSC during the Preliminary Engineering phase of the project. The purpose of the FLSSC will be to review issues that are critical to fire and life safety and security, to acquire input and concurrence from the state and local authorities having jurisdiction over the proposed designs to meet code requirements, and to ensure compliance with state and local fire code standards or fire/life safety hazard mitigation measures during the design phase. As the project moves into the Testing and Startup Phase the FLSSC will review

operating plans and procedures, results of after-action reviews following major emergency response incidents or exercises, and training programs for content appropriateness and effectiveness.

The single system FLSSC will focus on systemic, high-level, fire/life safety and security issues, including federal and state codes or requirements impacting the regional efforts. A goal of the system FLSSCs is to obtain concurrence from federal and state authorities with respect to fire and life safety and security concerns. The system FLSSC will include a representative from each regional FLSSC as well as representatives from state and federal agencies such as the Office of the State Fire Marshal, California Highway Patrol, Office of Emergency Services, the California Emergency Management Agency, CPUC, FRA, and DHS. The system FLSSC will be chaired by the Authority's Risk Manager. Meetings will be held regularly in Sacramento with agendas, minutes, and other support materials supplied by the committee co-chairs. Minutes and action items from the meetings will be conveyed to the regional FLSSCs and to the Safety and Security Program Committee for their consideration

Regional FLSSCs will focus on the CHSTS characteristics specific to their corridor segments (type/length of underground and elevated structures, access methods, terminals, etc.) to provide input with respect to local building codes or requirements that are in line with the emergency response characteristics and capabilities of the local agencies. A goal of the regional FLSSC is to obtain concurrence from local authorities with respect to the proposed designs and the code requirements of the state and federal authorities having jurisdiction. The regional FLSSC will be composed of appropriate representatives (e.g., Fire Marshal) from local emergency response agencies (fire, police, EMT) and will be chaired by the Authority's Risk Manager. Meetings will be held regularly at a location local to the regional corridor, with agendas, minutes, and other support materials supplied by the committee co-chairs. Minutes and action items from the meetings will be conveyed to the system FLSSC and to the Safety and Security Program Committee for their consideration. One representative from each regional FLSSC will be asked to participate in the system FLSSC. Consistent membership is critical to success. Each regional representative must be the same representative attending to System FLSSC matters and reporting results to their specific Regional Committee.

The FLSSC Charter, Technical Memorandum 500.04, can be found in Appendix E of this SSMP.

3.3.4 Program Change Control Board

Change control for the CHSTS will be in conformance with *PC2.04 Program Change Control Procedure*. The procedure includes a Change Control Board made up of Authority, PMT, and PMO representatives

3.3.5 Rail Activation Committee (RAC)

The Rail Activation Committee (RAC) will coordinate planning and process development efforts for the operational testing of the system and eventual startup of revenue service. The RAC will be multi-disciplinary in scope and will be established during the latter stages of the Construction Phase.

3.3.6 System Integration Testing Committee (SITC)

The System Integration Testing Committee (SITC) will coordinate the development of an integrated testing program. The SITC will plan for the effective and efficient testing of subsystems, and then the overall system, including ensuring that as testing progresses mitigations are taken to ensure the safety of the tests. The maturity of the various subsystems will be taken into account prior to full development and assurance that the systems are proven safe. The SITC will be multi-disciplinary in scope and will be established during the latter stages of the Construction Phase.

3.4 Safety and Security Responsibilities Matrix

The requirements, authority, and activities for safety and security will be integrated into the overall project management. At each stage of project advancement, there will be a process in place to ensure that the appropriate parties are aware of their safety and security responsibility associated with the project activity. The Safety and Security Responsibility Matrix (Table 3-1) lists the activities to be performed and assigns the responsibilities from the Preliminary Engineering phase through system Start-up phase.

Table 3-1 Safety and Security Responsibilities Matrix

Key Safety and Security Certification Steps	Preliminary Engineering Phase					Final Design Engineering Phase					Construction Phase					Testing/Startup Phase				
	AUT	S/S	PMT	CMT	DBC	AUT	S/S	PMT	CMT	DBC	AUT	S/S	PMT	CMT	DBC	AUT	S/S	PMT	CMT	OMC
Develop/Update Certifiable Elements and Hazards Log	A	P	S	-	-	-	A	S	S	P	-	A	S	S	P	-	A	S	S	P
Hazard and Vulnerability Analyses	A	P	S	-	-	A	P	S	S	S	A	P	S	S	S	A	P	S	S	S
Develop S/S Design Criteria	A	P	S	-	-	A	P	S	S	S	A	P	S	S	S	A	P	S	S	S
Develop V&V Certifiable Items Lists	A	P	S	-	-	-	A	S	S	P	-	A	S	S	P	-	A	S	S	P
Verification of S/S Certifiable Items Lists	A	S	P	-	-	-	A	S	S	P	-	A	S	S	P	-	A	S	S	P
Issue Phase Certificates of Conformance	A	P	S	-	-	-	A	A	S	P	-	A	A	S	P	-	A	A	S	P
Approve Phase Certs. Of Conformance	P	S	S	-	-	P	S	S	-	-	P	S	S	-	-	P	S	S	-	-

Abbreviations: AUT = Authority Safety & Security; S/S = PMT Safety & Security; PMT = Program Mgmt. Team
DBC = Design/Build Contractors; OMC = Operations & Maintenance Contractors; CMT = Construction Mgmt. Team
PE = Preliminary engineering Phase; FD = Final Design Phase; CN = Construction Phase
TS = Testing & Startup Phase

Responsibilities: P = Primary S = Supporting A = Audit - = None

4.0 HAZARD AND VULNERABILITY MANAGEMENT

4.1 Overview

A hazard is a condition or circumstance that could lead to an unplanned or undesired event which, when it occurs, can cause injury, illness, death, damage or loss of equipment or property, or severe environmental damage.

Threats are defined as specific intentional acts that will damage the system, its facilities, or its patrons. Threats include any intentional actions which detract from overall security. They range from the extreme of terrorist-initiated bombs or hostage-taking to more common events such as theft of services, pick pocketing, graffiti and vandalism. Vulnerability is defined as the susceptibility of the system to a particular type of security threat.

A formal process for the management of safety hazards and security threats and vulnerabilities will be used for the CHSTS. The purpose of the process is as follows:

- Identify and evaluate the effects of hazardous conditions and security threats and vulnerabilities on passengers, CHSTS personnel, CHSTS infrastructure and equipment in order to apply the Prevention Through Design principles identified in Section 5.1 of this SSMP;
- Define and evaluate countermeasures to eliminate or control the identified hazards and security threats and vulnerabilities;
- Provide timely notification of the identified hazards and threats and vulnerabilities to design personnel to resolve them;
- Document the development and incorporation of safety and security concepts during System development and implementation, demonstrating how an acceptable level of safety and security is to be achieved.

Managing safety hazards and security threats and vulnerabilities through identification, assessment, resolution, and tracking will be an essential function of system development from preliminary engineering through system start up with support by the PMT. This process will be initiated during the preliminary engineering (PE) phase. The PMT System Safety Manager will perform a Preliminary Hazard Analysis (PHA) and the PMT Security Manager a Threat and Vulnerability Assessment (TVA) upon final selection of the alignment and in the earliest stages of design. These processes will be coordinated through and reviewed by the SSPC.

The PHA will follow the methodology described in the FTA document *Hazard Analysis Guidelines for Transit Projects*. The TVA will follow the methodology in the FTA document *Public Transportation System Security and Emergency Preparedness Planning Guide*. Because of the sensitive nature of the security risk assessment, only those with a “need-to-know” will have access to the TVA, and the document will be considered Sensitive Security Information (SSI).

The development of the safety hazard analyses and security risk assessments will be coordinated with the appropriate engineering disciplines for the identification of applicable hazards/security risk issues and recommended control measures. Upon completion of PHAs and TVAs a Preliminary Hazard Analysis Report and Threat and Vulnerabilities Report will be prepared and submitted to the SSPC for review. The SSPC will elevate the reports to the Authority as appropriate to the processes described in Section 3.3.2.

As the System enters Final Design, the design/build contractors will review and update the CEHL, and work with the PMT System Safety and Security Manager to perform other analyses as warranted by local or site-specific conditions or designs. Any deviations to the Design Criteria will follow the procedures outlined in section 5.4. Other hazards or vulnerabilities may be identified during the normal course of work on the development of the CHSTS, including such activities as design reviews, construction inspection and testing, and start-up and integrated testing. Additional hazards or vulnerabilities identified during these activities will also require a hazard analysis or vulnerability assessment to be performed.

The SSPC will be responsible for reviewing and approving all hazard analyses and vulnerability assessments to ensure that significant safety hazards and security threats and vulnerabilities are identified and that the proposed countermeasures adequately resolve the issues. The SSPC will monitor the status of the identified hazards and vulnerabilities from initial identification through final resolution and closure in conformance with the V&V process and by utilizing reports from the V&V Requirements Management Tool database. Sensitive security issues will be tracked on a separate log per the CHSTS SSI Program.

4.2 Safety Analysis Processes

This section of the SSMP describes the requirements of safety analysis for the CHSTS and the processes the Program Management Team and all contractors (including design/build contractors) will use to identify, evaluate, and resolve potential hazards associated with the design, construction, testing and commissioning of the project.

The objective of safety analysis is to assess identified hazards in terms of the severity or consequence of the hazard and the probability of occurrence, and to find an acceptable resolution. Hazards shall be resolved through the *Prevention through Design* hierarchy of controls as identified in Section 5.1 of this SSMP. Hazards that cannot be eliminated in the design are to be controlled by providing safety devices, warning devices, and providing adequate training and written instructions to the high-speed rail system personnel to prevent accidents.

The safety analyses required are part of a formalized process to identify, eliminate and/or control hazards. Specifically, the safety analyses provide for the:

- Identification of hazards;
- Assessment of the severity and probability of occurrence of the potential hazard;
- Timely awareness of hazards for those who must resolve them; and
- Traceability and control of hazards through all phases of a system's life cycle.

Safety analyses are an essential part of the preventive and proactive aspect of the system safety program. Safety analyses primarily identify and describe hazards that might arise from flaws and fault conditions in the design and operation of a system or subsystem. Thus, a safety analysis is an important element in the development of a system in which hazards must be eliminated or controlled to an acceptable level.

4.2.1 Hazard Analysis Methodology

Safety analyses can be performed qualitatively or quantitatively. A qualitative analysis is a review of factors affecting the safety of a system. Possible conditions and events and their consequences are considered to determine whether they could cause or contribute to injury or damage. A quantitative analysis is a mathematical assessment of an actual or potential event, such as an accident. Quantitative evaluations can be used to establish absolute or relative frequencies of occurrence. A quantitative analysis will normally be accompanied, or preceded, by a qualitative analysis. Therefore, any mention of a quantitative analysis implies that a qualitative analysis has also been performed. The objective of the safety analysis, qualitative and/or quantitative, is to achieve maximum safety by eliminating or controlling all hazards posing an unacceptable or undesirable risk as measured by their combined hazard severity and qualitative frequencies of occurrence.

The types of analyses which may be required for the development of the CHSTS are described below.

- Preliminary Hazard Analysis (PHA) is typically the initial hazard analysis technique used during the system or subsystem design phase. A PHA is used to identify safety critical areas within the system and roughly evaluate hazards and begin to consider safety design criteria. PHA establishes the basis for the safety criteria in design, equipment, and performance specifications.

- Site-Specific Hazard Analysis (SiSHA) is an expansion of the PHA, conducted as the general design criteria and system requirements are applied to specific system and subsystem elements. An example would be a SiSHA for an elevated structure spanning the SR-99 highway in Fresno, applying the safety-critical criteria found in the Design Criteria to the specific characteristics and site conditions of this structure. SiSHA is generally performed during the Final Design, construction, and Testing/Startup Phases. The primary output of the SiSHA is the identification and evaluation of hazards and mitigations that are specific to the system element under consideration.
- Failure Modes and Effects Analysis (FMEA) is an inductive analysis used to identify equipment failures. It evaluates a system or subsystem to identify possible failures of each individual component in the system. The results or effects of the subsystem and component failures are then classified according to severity.
- Fault Tree Analysis (FTAn) is representative of the deductive process. The purpose of the Fault Tree Analysis is to provide a concise and orderly description of the various combinations of possible occurrences within the system that can result in an undesired event. This is the most rigorous of the hazard identification process and analyses and is typically performed for the most complex systems.
- Interface Hazard Analysis (IHA) is performed to identify design hazards in components and subsystems of a major system. IHA determines the functional relationships between the systems, subsystems, processes, components and equipment based solely on safety considerations and also identifies all elements in which a functional failure could result in a hazardous condition or accidental loss.
- Operating Hazard Analysis (OHA) is performed to determine all applicable operational safety requirements for personnel, procedures, and equipment throughout all phases of the system life cycle. Engineering data, procedures, and instructions developed from other safety analyses, the engineering design, and initial test programs are used to support this analysis.
- Software Hazard Analysis (SHA) will be used to evaluate software design, and related software and hardware documentation will be reviewed for safety-critical software-controlled functions. The analysis will review software and hardware failures that could cause the system to operate in a hazardous manner.

4.2.2 Interrelationships

To appreciate the utility of the safety analyses described in this document it is useful to understand their interrelationships and when they should be applied during the project life cycle. Table 4-1 displays the time frame in the life of a project when each safety analytical technique provides the most benefit. It should be understood that the number of in-process submittals of an analysis will vary and depend on the nature, complexity, and duration of the system contract and its life cycle.

Table 4-1 Project Life Cycle

Safety Analyses	Project Life Cycle				
	Planning	Preliminary Design	Final Design	Construction/ Procurement/ Installation	Integration Test/ Startup
Preliminary Hazard Analysis (PHA)	■				
Site-Specific Hazard Analysis (SiSHA)			■		
Failure Modes and Effects Analysis (FMEA)			■		
Fault Tree Analysis (FTAn)			■		
Interface Hazard Analysis (IHA)			■		
Operating Hazard Analysis (OHA)				■	
Software Hazard Effects Analysis (SHEA)	■				

4.2.3 Hazard Identification and Resolution Process

The process flow used for identifying hazards consist of review of the design and operational concepts, and incorporation of historical information and data from similar high-speed rail systems are identified in Table 4-2.

Table 4-2 Hazard Identification and Resolution Process

1. DEFINE THE SYSTEM
   - Define the physical and functional characteristics and understand and evaluate the people, procedures, facilities, equipment, and environment.

2. IDENTIFY HAZARDS
   - Identify hazards and undesired events
   - Determine the causes of hazards

3. ASSESS HAZARDS
   - Determine severity
   - Determine probability
   - Decide to accept risk or eliminate/control

4. RESOLVE HAZARDS
   - Assume risk or
   - Implement corrective action
     - Eliminate
     - Control

5. FOLLOW-UP
   - Monitor for effectiveness
   - Monitor for unexpected hazards

4.2.3.1 Hazard Resolution

As part of the hazard assessment process, hazards can be resolved by deciding to either assume the risk associated with the hazard or to eliminate or control the hazard. Mitigation of the risk associated with each hazard to an acceptable level shall be applied in the following order of precedence:

1. Avoidance
2. Elimination
3. Substitution
4. Engineering Controls
5. Warnings
6. Administrative Controls such as Operations and Maintenance Procedures
7. Personal Protective Equipment and Guards

4.2.3.2 Residual Hazard Risk Index

After the adoption of measures of mitigation the anticipated residual hazard risk index, expressed as the combined hazard severity and probability of occurrence, will be identified on the analysis sheet for each hazard. This will help evaluate the effectiveness of the corrective action and establish whether the residual hazard is acceptable.

Hazards identified as “acceptable with review” may be accepted in an “as-is” condition with no further design mitigation required. Operating and maintenance procedures must be developed, however, for periodic tests and inspections of the subject item to ensure an acceptable level of safety is maintained throughout the life of the system. The hazards and mitigations will be reviewed by the SSPC, with recommendation made to the SSEC for decision. Acceptance of the level of safety will be provided by the Authority through the SSEC, chaired by the Authority Chief Executive Officer.

4.2.3.3 Residual Risk Acceptance or System Disposal

Hazards identified as having an unacceptable and undesirable risk will be analyzed using logic network analyses (such as fault tree) to determine effectiveness of corrective action. Unacceptable and undesirable risk will be reduced to an acceptable level before design acceptance, or a decision must be made to accept the hazard or dispose of the system. The hazards will be reviewed by the SSPC, with recommendation made to the SSEC for decision. Acceptance of the level of safety or disposal of the system will be provided by the Authority through the SSEC.

4.2.3.4 Documentation

Appropriate support documentation used in the development of hazard analysis will be identified or referenced in detail as part of each analysis, including, but not limited to, the following:

- System description including modes of operation and tasks
- Schematics, drawing, block diagrams, lists of assemblies, parts and components addressed within each subsystem and system
- Documented reliability and safety data including failure rate data obtained from service use in identical or manifestly similar equipment in similar environment
- Documented reliability and safety data obtained from formal test results, conducted in similar applications
- Documented reliability and safety data obtained from formal analyses, conducted for equipment in similar applications

4.2.4 Hazard Category Definitions

The major output of the safety analyses is the identification and evaluation of hazards. It is important to provide a uniform interpretation of the severity and probability of the hazards. The following category definitions are used to develop the hazard analyses.

4.2.4.1 Hazard Severity

Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, system, subsystem or component failure, or malfunction. For the CHSTS, the hazard severity definitions are defined in Table 4-3.

Table 4-3 Hazard Severity Definitions

Hazard Category	Definition
I Catastrophic	Any hazard that can lead to: • Numerous fatalities • Numerous severe injuries • Severe damage or total loss to multiple railcars • Severe damage to rail infrastructure • Severe damage to another train or a fixed immoveable object (e.g., bridge abutment) • Other severe system loss causing all or a significant portion of the system unavailable for normal service for more than 5 calendar days • Severe environmental damage (including hazards associated with chemical, biological, radiological, nuclear and explosions)
II Critical	Any hazard that can lead to: • A fatality or multiple severe injuries • Severe occupational illness • Major but repairable damage to railcars • Major damage to rail infrastructure, but repairable within 5 calendar days to allow service to operate in the area • Other major system loss, but repairable within 5 calendar days to allow service to operate in the area • Major environmental damage (including hazards associated with the release of hazardous material into environment that may result in injury or death)
III Serious	Any hazard that can lead to: • Non-recoverable injuries or multiple minor injuries that require hospitalization and may lead to a fatality • Serious occupational illness • Serious but repairable damage to railcars • Serious damage to rail infrastructure, but repairable within 24 hours to allow service to operate in the area • Other serious system loss, but repairable within 24 hours to allow service to operate in the area • Serious environmental damage (including hazards associated with the release of hazardous material into environment that requiring evacuation)
IV Marginal	Any hazard that can lead to: • Recoverable (non life threatening) injuries that may require admittance to an emergency room for testing and/or hospital for observation • Minor occupational illness • Minor repairable damage to railcars • Minor damage to rail infrastructure, repairable within 2 hours to allow service to operate in the area • Other minor system loss, repairable within 2 hours to allow service to operate in the area • Minor environmental damage (associated with release of hazardous material into environment less than the EPA reportable amount)
V Negligible	Any hazard that can lead to: • Superficial injuries that may require first-aid treatment only • Less than minor occupational illness • Less than minor environmental damage (associated with hazardous material spill) • System shut down of less than 30 minutes

4.2.4.2 Hazard Probability

The assessment of the hazard should also include a probability of occurrence. Assigning a quantitative probability to a hazard is generally not possible early in the design or planning process. A qualitative hazard probability can be derived from research, analysis, and evaluation of historical safety data from similar systems. The hazard probability (frequency of occurrence) levels are defined in Table 4-4, which

includes a column on “Period of Occurrence (T) of an Event” that can be used as a guide in determining qualitative level of frequency of occurrence of a hazard.

Table 4-4 Hazard Probability Levels

Description	Level	Qualitative Definition	Period of Occurrence (T) of an Event
Frequent	A	Likely to occur frequently; continuously experienced in the fleet.	T < 2 months
Probable	B	Will occur several times in the life of an item; will occur frequently in the fleet.	2 months < T < 1 year
Occasional	C	Likely to occur sometime in the life of an item; will occur several times in the fleet.	1 year < T < 10 years
Remote	D	Unlikely, but possible to occur in the life of an item; unlikely but can reasonably be expected to occur in the fleet.	10 years < T < 30 years
Highly unlikely	E	So unlikely, it can be assumed occurrence may not be experienced. Failure of a series of risk control measures must happen before the event can occur.	T > 30 years

4.2.4.3 Hazard Risk Assessment and Acceptance Criteria

Hazard analyses establish hazard severity categories (I through V) and hazard probability levels (A through E) which are combined into a Risk Assessment Matrix to produce a Hazard Risk Index, reflecting the combined severity and probability ranking for each identified hazard. Risk Acceptance Criteria are applied to the identified hazards based on their Risk Assessment Code to determine acceptance of the risk or the need for corrective action to further reduce the risk. The Risk Assessment Matrix and Risk Acceptance Criteria are defined in Tables 4-5 and 4-6 respectively.

Table 4-5 Risk Assessment Matrix

Event Frequency of Occurrence	Event Severity				
	I (Catastrophic)	II (Critical)	III (Serious)	IV (Marginal)	V (Negligible)
(A) Frequent	1A	2A	3A	4A	5A
(B) Probable	1B	2B	3B	4B	5B
(C) Occasional	1C	2C	3C	4C	5C
(D) Remote	1D	2D	3D	4D	5D
(E) Highly unlikely	1E	2E	3E	4E	5E

Table 4-6 Risk Acceptance Criteria

Hazard Risk Index	Acceptance Criteria
1A, 1B, 1C, 2A, 2B, 2C, 3A	Unacceptable
1D, 2D, 3B, 3C	Undesirable (decision required SSEC)
1E, 2E, 3D, 3E, 4A, 4B	Acceptable with review by SSEC
4C, 4D, 4E, 5A, 5B, 5C, 5D, 5E	Acceptable

Hazards identified as “acceptable with review” may be accepted in an “as-is” condition with no further design mitigation required, however the hazard analysis must be reviewed and approved by the SSEC. See Section 4.2.3.3 for details.

4.2.4.4 Systems and Subsystems

A system is a composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement.

A subsystem is an element of a system that in itself may constitute a system. Depending on the nature and scope of the contract or subcontract, the connotation of system and subsystem may differ. For example, if the safety analyst conducts an Interface Hazard Analysis, the system would be the entire high-speed rail system and the interfacing subsystems, for example, could be high-speed rail system elements such as the passenger vehicle, traction power, train control, and communications. If the vehicle contractor conducts an IHA, the system would be the passenger vehicle and examples of subsystems could be the vehicle propulsion subsystem and friction brake subsystem. If the propulsion supplier conducts an IHA, the system would be the propulsion system and the subsystems could be the traction motors and the gear reducer and coupling.

4.2.4.5 System Mode

System mode is the state in which the system under analysis is assumed to be. The system may be in one of three states: normal (N); abnormal (A), which is a failure recovery mode (e.g., single track operation); or, emergency (E). The following is an explanation of the three possible system modes:

- NORMAL CONDITION (N): Refers to an operating condition wherein the high-speed rail system is operating under nominal design and operating conditions. Normal conditions mean that all systems are functional and the high-speed rail system is not under pre-existing degraded performance due to an existing malfunction
- ABNORMAL CONDITION (A): Refers to an operating environment wherein the high-speed rail system is operating under conditions of faults or malfunctions, which in and of themselves is not catastrophic or critical but degrades quality of service and possibly increases risk exposure. Abnormal conditions may require departure from the nominal operating conditions, and implementation of failure management and failure recovery strategies to continue revenue service with alternative measures or workarounds. Examples could be equipment malfunctions or maintenance constraints which require single-track operation on segment of track, or the temporary implementation of a manual block system in lieu of failed ATP equipment, to provide equivalent level of safety in lieu of failed equipment.
- EMERGENCY CONDITION (E): A life threatening situation posing clear and present danger such as fire/smoke on the vehicle, fire in a station, collision/derailment of the vehicle, bomb threat, etc.

4.2.5 Hazard Analysis Types

4.2.5.1 Preliminary Hazard Analysis (PHA)

The primary output of the PHA is the early identification and evaluation of hazards and mitigations on a high-level systems requirement basis. The following instructions are used in the development of the Preliminary Hazard Analysis (Sample PHA is shown in Figure 4-1).

PURPOSE	The purpose of the PHA is to provide an early assessment of the hazards associated with a design or concept.
PROCEDURE	The PHA identifies critical areas, hazards and criteria being used and considers: hazardous events, components, interfaces, environmental constraints, and operating, maintenance and emergency procedures. When possible, the corrective action should identify the approach(s) to be taken: design change, procedures, and special training and personnel qualifications.
RESULTS	The PHA will provide for verification that corrective or preventive measures or procedures are taken in safety reviews, modification of specifications, and generation of methods and procedures to eliminate, minimize or control hazards and provide inputs to the interface hazard analysis, operating hazard analysis and failure mode and effects analysis.
DOCUMENTATION	Document the analysis to show compliance with the specified safety and operational requirements, and provide for the tracking of actions and verifying effectiveness. A PHA Report will be developed where appropriate to document the analysis process for specific subsystem hazards.

Figure 4-1 Sample PHA

System: Infrastructure				**California High-Speed Train System**				**Prepared by:** John Cockle **Date**		
Subsystem: R-O-W, Generally				**Preliminary Hazard Analysis (PHA)**				**Reviewed by: Safety & Security Program Committee Date**		
PHA No. 1.1.1 **Rev No.** 0				DRAFT 11/25/2012				**Approved by: Safety & Security Executive Committee Date**		
General Description Derailment				**Hazard Cause / Effect**		**Hazard Risk Index**		**Corrective Action**		
No.	**Sys Mode**	**Site Speci-fic**	**Hazard Description**	**Potential Cause**	**Effect on Subsystem / System**	**Initial**	**Residual (Projected)**	**Controlling Measures and Remarks**	**Resolution / Reference**	**Notes**
4	Normal	Yes	Washout	Flooding, scouring	Derailment w/mass casualties, property damage, service interruption	I-B Unacceptable	I-E Acceptable w/Review	1) Perform hydraulics analysis and incorporate results into sub-grade design, slope protection and setting of profile. 2) Install scour protection (revetment or other structure) to protect sub-grade from water course. 3) Install culvert or bridge structure where crossing water course.	1) DM 10.5, DM 10.8.5.8 2) DM 8.4.3, DM 8.4.9	Identified 8/30/11. Improvement in frequency to *Highly Unlikely* , but not eliminated. No effect on severity of a derailment if it does occur.

Note – Figure 4-1 is a sample representation only. Refer to current PHA for identified hazards and controlling measures.

INSTRUCTIONS FOR COMPLETING THE PHA FORM:

- In System, enter the nomenclature of the applicable system element (e.g. Infrastructure, Train Control, Communications, Rolling Stock, etc).
- In Subsystem, enter the nomenclature of the subsystem as broken out from the system and which includes the item or hazard undergoing PHA.
- In PHA No., enter the PHA number for the subsystem element. This coding will be sequentially numbered by each Contractor for each subsystem and will be utilized for all related analysis.
- In Rev. No., enter the revision number of the PHA to indicate the latest status.
- In Prepared by _ Date _, the preparer will sign and enter the date of issue or revision of the analysis.
- In Reviewed by SSPC_ Date _, enter the date of review and SONO by the Safety and Security Program Committee.
- In Approved by SSEC_ Date _, enter the date of approval by the Safety and Security Executive Committee.
- In No., enter the reference number which uniquely identifies the high-speed rail system element and any identifiable element subsystem and item being analyzed.
- In System Mode, enter state of the system when the failure mode or hazardous condition occurs.
- In HAZARD DESCRIPTION, describe an immediate condition which could lead to an accident involving potential injury, death or equipment damage.
- In POTENTIAL CAUSE, enter the most likely primary and secondary causes that can potentially contribute to the presence of the hazard.
- In EFFECT ON SUBSYSTEM / SYSTEM, describe the effect that the hazardous condition may have on the system element or its element subsystem in terms of safety (e.g. delay, inconvenience, injury, damage, fatality, etc.)
- In HAZARD RISK INDEX, enter a combination of the qualitative measure of the worst potential consequence resulting from the hazard, and its probability of occurrence (e.g., IA, IIB, etc.), under the following conditions:
    - In INITIAL, enter the designation for hazard risk index estimated prior to implementation of the controlling measures, considering the condition of the subsystem element if no measures of mitigation were applied.
    - In RESIDUAL (PROJECTED), enter the designation for hazard risk index estimated following the adoption/implementation of the proposed controlling measures. This may result in reduction of either the probability of occurrence or the severity of the hazard, or both.
- In CONTROLLING MEASURES AND REMARKS, describe the proposed measures of mitigation that can be applied to prevent or reduce the severity and probability of the hazard under analysis.

- In RESOLUTION / RESOLUTION, describe changes made or steps taken relative to design and/or procedures, training, etc., to eliminate or control the hazard. The identified reference should be as specific as possible for verification purposes.
- In NOTES, identify the date that the hazard was initially analyzed, any subsequent analysis, and other items that support or describe the analysis process.

4.2.5.2 Site-Specific Hazard Analysis (SiSHA)

The SiSHA is conducted as the general design criteria and system requirements are applied to specific system and subsystem elements within a defined geographic area. The standard SiSHA segment will be one mile in length, but can be shorter if specialized conditions require. SiSHA is systemic in that it includes ALL hazards and mitigations that are found within the segment under consideration, analyzing the relationship between the various hazards and mitigations. SiSHA is performed when the final alignment is identified during the Preliminary Engineering Phase and in advance of the Final Design, Construction, and Testing/Startup Phases. The primary output of the SiSHA is a validation of the PHA mitigations in relation to the segment under consideration, and the identification and evaluation of hazards and mitigations that are specific to the segment under consideration.

The instructions for completing the SiSHA form are the same as for the PHA form, as identified in Section 4.2.5.1 of this SSMP.

Figure 4-2 Sample SiSHA

Section:	CP01-193 MP 192.0 - MP 193.0	CALIFORNIA HIGH-SPEED TRAIN SYSTEM Site-Specific Hazard Analysis							Prepared by: John Cockle Date DRAFT 8/16/12
North Limit:	11000+00	Design Milestone: RFP HSR 11-16, Addendum 3, 6/29/12							Reviewed by: SSPC Date
South Limit:	11052+80								
Description:	Fresno station south to approximately South Cherry Ave. Includes 4-track HST trainway for station, plus to additional refuge tracks south of the station. Includes 1 new Tulare Street overpass/underpass, 1 new Ventura Street overpass and 2 existing SR-41 overpasses. UPRR located on east side of trainway.								Approved by: SSEC Date
PHA Number	Hazard Description	Applicable Limits		Effect / Consequence	Initial Risk	Residual Risk	Applied Mitigations	Other Affected Hazards	Notes
1.1.1.4	Derailment - Washout caused by flooding or scouring	11000+00	11052+80	N/A	N/A	N/A	1) Perform hydraulics analysis and incorporate results into sub-grade design, slope protection and setting of profile.	N/A	No water courses crossed.
1.1.1.5	Derailment - Slide caused by hillside movement, storm water runoff	11000+00	11052+80	N/A	N/A	N/A	1) Perform geotechnical analysis to evaluate slope stability that could effect the HSR trackway. 2) Perform hydraulics analysis and incorporate results into sub-grade design, slope protection and setting of profile.	N/A	No adjacent hillsides
1.1.1.6	Derailment - Seismic activity.	11000+00	11052+80	Derailment w/mass casualties, property damage, service interruption	I-D Undesirable	III-E Acceptable w/Review	1) Perform seismic analysis to determine potential limits of ground movement at the location. 3) Install earthquake monitoring devices at regular intervals for notification of seismic event. 4) Establish an operational response based upon notification of a seismic event. 5) Identification and monitoring of potential hazardous locations.	1.2.1.3 1.2.2.1 1.2.3.1 1.2.4.5 1.2.4.6	Trainway does not cross an active fault zone at this location.
1.1.1.7	Derailment - High winds	11000+00	11052+80	Derailment w/mass casualties, property damage, service interruption	I-B Unacceptable	IV-E Acceptable	1) Perform wind analysis for effects on vehicles and operations. 2) Install weather stations at regular intervals to monitor wind conditions. 3) Develop operational responses to extreme wind conditions.		Not an area of high winds.
1.1.2.2	Collision - Non-HSR train enters HSR trackway from adjacent exclusive corridor.	11000+00 - 11026+00	11026+00 (Required) 11052+80 (Decision by CHSRA)	Derailment w/mass casualties, property damage, service interruption	I-C Unacceptable	I-E Acceptable w/Review	1) Install intrusion prevention measures appropriate to site-specific conditions. 2) Install an intrusion detection system. 3) Develop operational responses to intrusion detection.	1.1.2.5 1.1.2.10 1.1.4.2 1.1.5.1 1.1.5.2 1.2.1.4	Intrusion barrier in compliance with TM 2.7.1 required account Relative Hazard Frequency Assessment = 137.11 (Limits 11000+00 to 11026+00). RHFA = 90.40 (Undesirable-decision required by Authority) for limits 11026+00 to 11052+80. Primary reason for these RHFA ratings is close proximity of UPRR to CHST track centers, plus special trackwork and switching activities associated with UPRR and SJVR interchange. See ARHRAM report for CP01.

4.2.5.3 Failure Mode and Effects Analysis (FMEA)

PURPOSE

The purpose of the FMEA is to determine the results or effects of item failures on a system operation and to classify each potential failure according to its risk index (severity and frequency of occurrence). The goal is to provide an early identification of failures with unacceptable and undesirable risks so that they can be eliminated or minimized through appropriate actions at the earliest possible time.

PROCEDURE

Variations in design complexity and available data will generally dictate the analysis approach to be used. There are two primary approaches for accomplishing an FMEA, the hardware

approach and the functional approach.

The hardware approach is normally used when hardware items can be uniquely identified from schematics, drawings, and other engineering and design data. The hardware approach is normally utilized in a parts-level up fashion (bottom-up approach); by listing individual hardware items and analyzing the effect of their possible failure modes on the entire system and its subsystems.

The functional approach is normally used when hardware items cannot be uniquely identified or when system complexity requires analysis from the initial indenture level downward through succeeding indenture levels (top-down approach). The functional approach recognizes that every item is designed to perform a number of functions that can be classified as outputs. The outputs are listed and their failure modes analyzed.

The FMEA may be performed as a hardware analysis, a functional analysis, or a combination analysis depending on the design detail available.

The FMEA will examine the system element by element, to evaluate the system for safety hazards and ultimately to assess risk. Each identified failure mode will be assigned a severity classification. A probability of occurrence will also be assigned in accordance with MIL-STD-882E The resulting risk index will be utilized during design to establish priorities for corrective actions. The FMEA will be reviewed on a continuous basis to verify that design modifications do not add hazards to the system.

To perform a FMEA, the following process should be implemented:

- Identify all major system components, functions, and processes
- Determine consequences of interest
- Determine the potential failure modes of interest
- Specify effects of failures of system
- Identify safety provisions to control hazards and failures
- Identify detection methods for failures
- Establish overall significance of each failure

RESULTS

The FMEA will provide information to evaluate identified hazards, identify safety critical areas and provide inputs to safety design criteria and procedures with provisions and alternatives to eliminate or control all unacceptable and undesirable hazards based on their combination of severity and probability of occurrence, and to identify critical items.

DOCUMENTATION

Document the analysis to show compliance with specified system safety requirements and to track the corrective action.

4.2.5.4 Fault Tree Analysis (FTAn)

PURPOSE

The Fault Tree Analysis (FTAn) is a deductive procedure used to determine the various combinations of hardware and software failures and human errors that could cause undesired events (referred to as top events) at the system level. The FTAn has much use because of its ability to distinguish between those events that must occur (represented by an AND gate) and those that simply can occur (represented by an OR gate) in order for the top event to occur. The analysis thus helps to identify potential causes of system failures before the failures actually occur. The deductive analysis begins with a general conclusion, then attempts to determine the specific causes of the conclusion by constructing a logic diagram called a fault tree. After completing an FTAn, efforts can be directed to improve system safety.

PROCEDURE

The FTAn will be conducted on unresolved, undesirable, or unacceptable hazards identified in other safety analyses. Following procedure will be used to do a comprehensive FTAn:

1. Define the undesirable/unacceptable hazard, and write down the top level event.
2. Using technical information and professional judgments, determine the possible reasons for the top level event to occur. These are level two elements because they fall just below the top level event in the tree.
3. Continue to break down each element with additional gates to lower levels. Consider the relationships between elements to help decide proper selection of the logic gate.
4. .Finalize and review the complete diagram. The chain can only be terminated in a basic fault: human, hardware software.
5. If possible, evaluate the probability of occurrence for each of the lowest level elements and calculate the statistical probabilities from the bottom up.

RESULTS

The information charted on a fault tree provides a qualitative analysis by demonstrating how specific events will affect an outcome. If probability data is known for these events, then the FTAn can also provide quantitative information to further evaluate the likelihood of achieving the top event. Once developed, the fault areas that are responsible for yielding an undesired event can be further evaluated.

DOCUMENTATION

Document the analysis to show compliance with specified system safety requirements and to track the corrective action.

4.2.5.5 Interface Hazard Analysis (IHA)

PURPOSE	The IHA identifies and assesses existing or potential hazards between subsystems and systems and their effect on overall System safety and operations. The emphasis is on interfaces. Through the early identification of existing or potential hazards, corrective action(s) can be taken to eliminate or control unacceptable and undesirable hazards, based on the combination of their hazard severity and probability of occurrence.
PROCEDURE	The IHA is conducted on the critical interrelationships of each subsystem and system to determine the cause and effect of possible independent, dependent and simultaneous failures that could present a hazardous condition, including failures of safety devices. When the IHA indicates a potential problem, it is made known to the responsible engineer in order to initiate a design review. The IHA will be reviewed on a continuous basis to verify that design modifications do not add hazards to the system.
RESULTS	The IHA provides for the identification and correction of possible hazards associated with subsystem and system failures. The IHA provides inputs to design reviews, maintainability, reliability and system safety and system operations.
DOCUMENTATION	Document the analysis to show compliance with specified system safety requirements and to track the corrective action.

4.2.5.6 Operating Hazard Analysis (OHA)

PURPOSE	The purpose of the OHA is to identify and analyze hazards associated with personnel and procedures during production, installation, testing, training, operations, maintenance and emergencies.
PROCEDURE	The OHA will be conducted on all tasks and human actions, including acts of omission and commission, by persons interacting with the system, subsystems and assemblies at any level. When the OHA indicates a potential safety hazard, it will be made known to the responsible engineer, in order to initiate a design review or a system safety working group action item. The OHA will be reviewed on a continuous basis to provide for design modifications, procedures, testing, etc., that do not create hazardous conditions.

RESULTS	The OHA will provide for corrective or preventive measures to be taken to minimize the possibility that any human error or procedure will result in injury or system damage. The OHA will provide inputs for recommendations for changes or improvements in design or procedures to improve efficiency and safety, development of warning and caution notes to be included in manuals and procedures, and the requirement of special training of personnel who will carry out the operation and maintenance of the system.
DOCUMENTATION	Document the analysis to show compliance with specified system safety and operational requirements.

4.2.5.7 Software Hazard Effects Analysis (SHEA)

PURPOSE

The Software Hazard Effects Analysis (SHEA) is a software design evaluation and validation tool used to identify errors generated from incorrect or inadequate specifications of software functions. A software fault causing a resultant harmful system function is a software hazard.

Software faults can be described in three forms:

- Error generated through coding the software
- Faults due to incorrect software specifications implemented by the function developer
- Faults due to hardware failures that affect changes in coding software

A software hazard can be any of four types:

- An undesired signal causing an unwanted event
- An undesired signal causing an out-of-sequence event in the response
- An undesired signal preventing the occurrence of a necessary action or response
- An undesired signal causing an event to be out of tolerance

The SHEA concentrates on potential safety problem areas in the software. The purpose of the SHEA is to provide an early study of the software design for possible hazards and to initiate appropriate actions to eliminate/ control hazards.

PROCEDURE

The initial step in the analysis is to identify the safety critical areas of the system and their functional paths. These paths may contain hardware as well as software elements. Focus the analysis on the software functions within each system functional flow path. Whether the coded instructions are stored in software or firmware, analysis of the system in question for hazardous occurrences should include an analysis of the stored coded instructions.

The SHEA will be conducted on identified software fault conditions, and will proceed from a qualitative to a quantitative analysis as the design develops. When the SHEA indicates a potential problem, it will be made known to the responsible engineer in order to initiate proper action. The SHEA will be reviewed on a continuous basis to verify that software design

	modifications do not add hazards to the system. The SHEA should be developed in conjunction with FMEA.
RESULTS	The SHEA will provide information to evaluate identified software related hazards, identify safety critical areas in software design and provide inputs to safety design criteria and procedures. The latter will include provisions and alternatives to eliminate or control all unacceptable and undesirable software related hazards based on their combination of severity and probability of occurrence, and to identify critical items.
DOCUMENTATION	Document the analysis to show compliance with the specified system safety requirements and to track the corrective action.

4.3 Security Risk Assessment Process

Planning in advance of day-to-day passenger rail crimes, terrorist acts, or other security incidents is essential to providing CHST passengers and employees with a safe and secure environment. A breach in security may result in serious injuries or death, destruction of property and facilities, and/or the inability to continue CHSTS operations to the region.

Adopting a methodology that involves periodic assessment is consistent with the requirement of the system security lifecycle and ISO 31000 Risk Management standard.

In order to ensure that the Authority has considered security risks, such as crime or acts of terrorism, it is crucial to apply a methodological approach and process to security risk management. The risk assessment process that will be used, illustrated in Figure 4-3, includes the following:

- Identify the key assets,
- Identify the threats,
- Identify the vulnerabilities,
- Identify the likelihood ,
- Identify the consequence/impact,
- Assign the initial risk index as the basis for future risk decision criteria,
- Identify potential mitigation measures/countermeasures and
- Determine residual risk after implementation of countermeasures.

Figure 4-3 Security Risk Assessment Process.

To evaluate the susceptibility to potential threats and to design corrective actions that can reduce or mitigate the risk of serious consequences from a security incident, a Threat and Vulnerability Assessment (TVA) will be initiated during the preliminary phases of the CHSTS. The assessment will be reviewed and updated at each subsequent phase.

The TVA process will identify the likelihood of specific threats that may endanger railroad assets (people, property and information); the potential vulnerabilities associated with the design of the CHSTS; and mitigation efforts that can be designed into the CHSTS to reduce the risk and to minimize the consequences of identified potential criminal and terrorism activities. It will also identify future security training needs of transit personnel and the necessity for security procedures. The Security Risk Assessment will be protected under Sensitive Security Information (SSI) and shared *only* with those persons with a need to know.

4.3.1 Assets

4.3.1.1 Identification

Assets are defined as people and property. System assets include the following:

- People – passengers, employees, visitors, contractors, vendors, surrounding communities, and others who come into contact with the transit system
- Property – fixed infrastructure, rolling stock, software,
- Information – plans, procedures, network information, passwords and access codes

Assets associated with the CHSTS will be identified during the TVA process and included as a listing in the Threat and Vulnerability Assessment Report.

4.3.1.2 Criticality Determination

Assets will be prioritized in terms of criticality. Most weight will be given to those assets that present the greatest threat to life safety or service disruption. In making this determination, consideration will be given to the following:

- Impact on CHSTS passengers, employees, and first responders
- Impact on CHSTS operations
- Economic value of the asset, including current and replacement value
- Intrinsic value of the asset to a potential adversary
- Asset location relative to other critical asset

4.3.2 Identification of Threats

Threats are defined as deliberate actions intended to cause injury or death to people or damage or loss of critical assets. The threats (or attack types) to the CHSTS will generally be the same as those faced by other public transportation networks. Threat is the combination of both intent and capability of a threat actor or threat source to realize a threat or attack against an asset. It is possible to separately analyze the intent and the capability but this type of analysis requires specific information and intelligence about specific threat actors.

As part of the security risk management system it is important to understand target attractiveness. Target attractiveness varies depending upon threat actor motivations and goals, but in general the following criteria are useful in determining the potential for target selection:

- Potential for public impact, damaging the society and ecosystem as a whole;
- Lack of target protection and does the target follow predictable patterns;
- Potential for mass casualties;
- Potential for global significance or visibility to either the threat actor or the target;
- Target permanently or frequently available;
- Potential for major political or economic impact;
- Potential for economic gain;
- Ease of accessibility;
- Perceived “Iconic” status.

Determination of security threat is always evolving and requires analysis to be based on the past performance of threat actors, both successful and attempted. Historical data, from reliable open source

information, of manifested threat events across national and international transit systems provides accurate data to enable security threats to the CHSTS assets and systems to be established.

The series of tables below illustrate examples of threat categories (Table 4-7), crime categories (Table 4-8), and threat types (Table 4-9).

Table 4-7 Threat Category Examples

Threat Category	Sources
Criminal	Petty crime Organized crime Current/former staff
Terrorism	Domestic extremist groups Transnational extremist groups Single-issue groups
Hostile State	Military State-sponsored hostile actors

Table 4-8 General Crime Categories and Examples

Threat Category	Crime Types within Category
Crimes against Persons	Assault, homicide, robbery, theft
Crimes against Property	Arson, cargo theft, vandalism, burglary
Other Crimes committed on Transit Property	Organized crime presence – infiltrating rail system, using rail system to move contraband, drugs, prostitution, fare evasion, trespass

Table 4-9 Threat or Attack Types Examples

Threat Type	Types within Category
Explosives	Military explosive, Improvised Explosive Device (IED), Vehicle-Borne Improvised Explosive Device (VBIED), Personnel-Borne Improvised Explosive Device (PBIED)
Chemical	Toxic Industrial Chemicals, and Poisons
Arson	Incendiary Devices
Small Arms Attack	Use of standard firearms and other weapons
Standoff Attack	Weapons with high-energy explosives that are designed to hit and penetrate heavily protected objects from a distance.
Cyber Attack	Viruses, Worms and Trojan Horses
Hoax Call or Device	Intentional false alarm or threat

As stated previously, threat is based upon the combination of intent and capability. Table 4-10 below provides the threat rating matrix based and Table 4-11 provides the threat ratings and their descriptions.

Table 4-10 Threat Rating Matrix (Intent x Capability)

INTENT	CAPABILITY				
	Similar exploit has been used	Operational capability confirmed by credible evidence	Some evidence that operational capability exists; not confirmed	No evidence of operational capability but feasibility confirmed	No evidence and even feasibility unconfirmed
Tactic has been used in the past and a similar attack may be planned	**Very High**	**Very High**	**High**	**Medium**	**Low**
Tactic has been used before and it is credible that it is being considered for further use	**Very High**	**High**	**High**	**Medium**	**Low**
Tactic has not been used before but is under consideration	**High**	**High**	**Medium**	**Medium**	**Low**
Tactic has not been used before but it may be under consideration	**Medium**	**Medium**	**Medium**	**Low**	**Very Low**
Tactic has not been used before and is not known to be under consideration	**Low**	**Low**	**Low**	**Very Low**	**Very Low**

Table 4-11 Threat Rating and Definitions

Threat Rating	Threat Rating Definition
VERY HIGH	Significant and proven threat present based upon demonstrated intent and demonstrated capability
HIGH	Threat present based upon stated/demonstrated intent with demonstrated capability.
MEDIUM	Medium level threat exists based upon either strong intent or some degree of stated/demonstrated capability.
LOW	General threat exists and should be monitored – no proven intent or demonstrated capability
VERY LOW	General threat may exist with intent and capability feasibility unconfirmed

For purposes of the CHST System, threat of terrorist activity will be based on information provided by DHS/TSA and other credible sources. For other threats, including crime and quality of life incidental threats, the Security Risk Assessment will review crime data provided by law enforcement in the adjacent areas, and open source data of criminal threats for other rail systems.

4.3.3 Scenario Analysis

Scenarios are the outcome of pairing specific assets with specific threats. An explosive device at a rail station provides a scenario that can be evaluated to identify the vulnerabilities that may make the rail station, an identified asset, susceptible to an attack. Scenario development also identifies impacts of threats on critical assets and promotes mitigation strategies and capability needs. The scenarios are intended to represent credible, real-world events and, as such, will be derived primarily from other operating systems' experiences, FTA and TSA resource documents, and local crime report information.

4.3.4 Identification of Vulnerabilities

Vulnerability is defined as any weakness, flaw or condition that allows and/or can be exploited, for the successful realization of a potential threat against the CHSTS. In general, vulnerability conditions allow access to an asset in order to be attacked. As the threat environment is ever changing, vulnerabilities to different threats and attack methods may also change, which requires updated review of the threats, vulnerabilities and the consequences. However, by addressing known vulnerabilities and therefore limiting the associated consequences of a potential threat, the likelihood of having to make significant changes is reduced for future updates.

Vulnerability conditions can be classified into two different types, physical, and procedural. A physical vulnerability condition is an actual physical deficiency, flaw, or absence of physical measures designed to deter, detect, delay, and/or respond against a breach or unauthorized access to an asset. A procedural vulnerability condition relates to the existence, implementation, legality, and oversight of policies and procedures, which are designed to deter, detect, delay, or respond against a breach or unauthorized access to an asset.

Successful execution of an attack type is dependent upon the presence of either a physical vulnerability, or a procedural vulnerability, or both. By identifying the physical and procedural conditions that contribute to a certain threat type and attack method, it is possible to start developing general mitigation strategies to address the vulnerability and therefore reduce the likelihood and/or consequences of a successful attack.

In a new project, the assumption is that the system is completely without mitigations measures, but takes into account typical operating features and assets. Any countermeasures that might impact a perceived vulnerability will be recommended for implementation in to the design and construction. Assessments performed on existing systems look for the weaknesses in an existing design or system.

Table 4-12 details the vulnerability levels used as part of the vulnerability determination.

Table 4-12 Vulnerability Levels and Description

Vulnerability Level	Assessment Criteria
Very High	• Non-existent advanced physical and procedural mitigation measures • Inadequate existing mitigation measures; and will likely fail to deter, detect, delay, or respond to a security risk • No security awareness culture present • No business or operations contingencies to manage security events and recover. Severe disruptions are likely
High	• Some physical and procedural mitigation measures, but ineffective at deterring, detecting, delaying, or responding to advanced security risks • More than 50% of existing mitigation measures are likely to fail to deter, detect, delay, or respond to a basic security risk • No security exercises performed or planned • Few contingencies/plans are in place for business and operations recovery. Significant disruptions likely
Moderate	• 50% of advanced physical and procedural mitigation measures are effective with remaining measures likely to fail to deter, detect, delay, or respond to a security risk • Existing mitigation measures are capable of deterring, detecting, delaying, and responding to basic security risks • Exercise program exists and exercises are performed for select areas • Basic security awareness culture • Contingencies/plans are in place across most but not all key areas of business and operations, but require improvement. Some disruptions are likely
Low	• 50% - 80% of advanced physical and procedural mitigation measures are effective but some improvements are required • Existing mitigation measures are capable of deterring, detecting, delaying, and responding to basic security risks • Procedures and evidence (records) of audit and review of existing security measures • Exercise program exists and exercises are performed for select areas • Cultivation of security awareness culture is a primary objective of management • Business and operations contingencies plans are in place for all key areas to manage security events and recover
Very Low	• 80% or higher effectiveness of advanced physical and procedural mitigation measures to deter, detect, delay, and respond to security risks and are sustainable • Procedures and evidence (records) of audit and review of existing controls • Exercise program exists and exercises are performed for select areas • Security awareness culture is integrated into all business activities • Comprehensive contingency plans in place across entire business and operations to manage most identified disruptions

4.3.5 Determining Likelihood

Likelihood is the combination of threat and vulnerability. Table 4-13 is a matrix that describes the combination of the threat and vulnerability to create the likelihood rating and index.

Table 4-13 Likelihood Determination Matrix (Threat x Vulnerability)

Threat	Vulnerability				
	Very High	High	Moderate	Low	Very Low
Very High	Almost Certain	Almost Certain	Highly Likely	Likely	Likely
High	Almost Certain	Highly Likely	Highly Likely	Likely	Possible
Medium	Highly Likely	Likely	Likely	Possible	Possible
Low	Likely	Likely	Possible	Possible	Remote
Very Low	Possible	Possible	Possible	Remote	Remote

The likelihood is based upon the below definitions in Table 4-14.

Table 4-14 Likelihood Rating and Definitions

Likelihood Rating	Likelihood
	Characteristics
Almost Certain A	Vulnerability exists and threat is proven and demonstrated. Threat realization can be expected to occur during the system's operational phases
Highly Likely B	Vulnerability exists and threat is proven although may not be demonstrated. Threat realization may be expected during system's operational phases
Likely C	Some vulnerability exists and threat has some resource, experience, and skill, though may not be demonstrated. Threat realization may occur during the system's operational phases
Possible D	Limited vulnerability exists and threat may be under resourced and may lack experience and skill, should not occur during the system's operational phases
Remote E	Limited vulnerability exists or threat has not been proven or demonstrated, not expected during the system's operational phases

4.3.6 Determining the Consequence

Consequence is the assessed impact and severity of a successful threat against an asset, the system, or network. Consequence is measured by the level of impact on primary areas of people, equipment or service and finances. Reputational impacts can also be assessed. Examples of consequences include injuries to the public or to CHSTS personnel, loss of equipment causing financial losses, and disruption to CHSTS operations. Reputational damage occurs when the system is considered unsafe or dangerous, impacting ridership, and funding. Severity categories are defined to provide a qualitative measure of the result of a security breach and are summarized in Table 4-15.

Table 4-15 Consequence Ratings and Assessment Criteria

Severity Rating	CHARACTERISTICS			
	People	**Equipment or Services**	**Financial**	**Reputational**
Catastrophic I	Several deaths and/or numerous severe injuries	Total loss of equipment or system interruption requiring months to repair	Estimated loss in excess of $5 million	Ongoing international, national media coverage, severe reputational damage, government intervention, Weeks - Months
Critical II	Low number of deaths (less than 3) and/or severe injuries	Significant loss of equipment or system interruption, requiring weeks to repair	Estimated loss from the incident expected to range from $500,000 to $5 million	Prolonged national and local media, serious reputational damage, sustained government involvement, Days-Weeks
Moderate III	Possible severe injury or several minor injuries	Loss of equipment or system interruption, requiring seven or less days to repair	Estimated loss from the incident expected to range from $50,000 to $499,999	Adverse national and local media coverage, reputational damage, government involvement
Minor IV	Possible minor injuries or illness	Minor loss of equipment, no system interruption, less than 24 hours to repair	Estimated loss from the incident expected to be minor, $1000 to $49,999	Local media coverage and some reputational damage
Negligible V	No injuries or illness	Minor damage to equipment, no system interruption, no immediate repair necessary	Estimated loss less than $1000	No adverse media coverage or reputational damage

4.3.7 Security Risk Criticality Matrix

The consequence, or severity, of a threat and the likelihood of occurrence will be combined into a risk level criticality matrix. The consequences will be assessed both in terms of severity of impact and probability of occurrence for a given threat. The criticality matrix organizes the resulting consequences into categories of high, serious, and low. The matrix will help to prioritize risk to focus available resources on the most serious threats requiring resolution while effectively managing the available resources. The Security Criticality Matrix is shown in Table 4-16.

Table 4-16: Security Risk Criticality Matrix (Likelihood X Consequence)

Consequence Severity	Likelihood				
	Almost Certain A	Highly Likely B	Likely C	Possible D	Remote E
Catastrophic – 1	Very High 1A	Very High 1B	High 1C	High 1D	Moderate 1E
Critical – 2	Very High 2A	High 2B	High 2C	Moderate 2D	Moderate 2E
Moderate – 3	High 3A	High 3B	Moderate 3C	Moderate 3D	Low 3E
Minor – 4	Moderate 4A	Moderate 4B	Moderate 4C	Low 4D	Very Low 4E
Negligible – 5	Low 5A	Low 5B	Low 5C	Very Low 5D	Very Low 5E

Source: Adapted from FTA's Public Transportation System Security and Emergency Preparedness Planning Guide

Once the risk rating is determined for each security risk to each identified asset, then the risk index at Table 4-17 can be used to determine and prioritize the resources and financial justification for risk treatment.

Table 4-17: Security Risk Index

Risk index	Risk Rating	Action Required
1A, 1B, 2A	VERY HIGH	Risk must be immediately mitigated and constantly monitored
1C, 1D, 2B, 2C, 3A, 3B	HIGH	Risk must be treated and monitored
1E, 2D, 2E, 3C, 3D, 4A, 4B, 4C	MODERATE	Risk should be managed and reduction strategies implemented
3E, 4D, 5A, 5B, 5C	LOW	Risk may be accepted after a risk review by the SSEC
4E, 5D, 5E	VERY LOW	Risk would normally not be treated

Source: Adapted from FTA's Public Transportation System Security and Emergency Preparedness Planning Guide

4.3.8 Countermeasure Development

After determination of the risk, countermeasures or corrective actions are developed that can mitigate or eliminate the risk. Effective countermeasures can either be design or procedural or a combination. Examples of design or engineered countermeasures include:

- Installing physical barriers designed to reduce the asset's vulnerability to unauthorized access, explosive, or other incendiary attacks
- Installing integrated intrusion detection and alarm systems throughout key facilities
- Installing chemical, biological, radiological and/or nuclear detection devices at facility and station locations

Procedural or Administrative countermeasures include:

- Increasing the frequency of security patrols at key asset locations
- Increasing security-related training to improve the abilities of employees to identify suspicious packages or activities
- Conducting emergency exercises and drills involving security-related scenarios
- Developing working groups and information exchange committees with local law enforcement and emergency response agencies.

During the development of countermeasures, consideration will be given not only to the initial costs of procurement and implementation, but also to the associated maintenance costs and expected level of effectiveness at eliminating or controlling the threat and/or vulnerability. Cases where conditions may be exacerbated, such as special events, will be taken into account. During these conditions, ridership is likely to be greater than normal and may impact the effectiveness of the countermeasure.

4.3.9 Residual Risk

Residual risk refers to the risk remaining after application of the countermeasures. If the residual risk has not been reduced to an acceptable level, additional countermeasures or mitigation strategies must be considered.

4.3.10 Reporting

The assessment details are captured in worksheets or tables which define the major elements of specific scenarios. An example of a TVA worksheet is shown in Figure 4-4.

Figure 4-4 Security Risk Worksheet Example

1.1.1 Fire

CALIFORNIA HIGH-SPEED RAIL SECURITY RISK ASSESSMENT		
Prepared by: Date:	Reviewed by: Date:	Approved by: Date:
Asset: Stations	Risk Assessment No: 4.1.3	Rev. No.:
Potential Threat	Fire	
Target	• Stations • Rail system infrastructure • Commuters and rail employees	
Tactical Delivery of Device	• Improvised Incendiary Device (IID) • Flammable fluids, liquids, or gases	
Potential Effects	• Disruption of rail service for prolonged periods of time • Damage or loss of train station and infrastructure short- to medium-term • Reduced ridership/farebox revenues • Economic disruption to surrounding area • Damage or loss of surrounding community area enterprises • Financial impact to clean-up effected area(s) • Death and/or injury	
Initial Security Risk Index		
Countermeasures	• Eliminate concealment areas at stations • Construct stations with clear lines-of-sight • Construct stations with non-combustible materials • Defined public space and restrict access to non-public space • Provide adequate lighting of station and approach area(s) • Monitor and record all station areas with CCTV • Conduct periodic and random security/law enforcement patrols • Train staff in security awareness practices to recognize, report, and respond to suspicious activities and packages • Schedule and conduct fire response drills and exercises • Implement "Transit Watch" public outreach and awareness campaign for reporting suspicious activity (people, vehicles, packages, etc) • Install station telephones/call-for-aid • Install and maintain firefighting equipment; • Establish station manager posts.	
Residual Security Risk Index		
Certification Log Tracking Reference		

4.4 Verification and Validation Documentation

Each identified safety hazard and security risk will be managed to resolution through the Verification and Validation (V&V) methodology and documented in the Requirements Management Tool database system adopted by the CHSTS. The V&V methodology and documentation requirements are described in Section 7.0 of this SSMP.

5.0 DEVELOPMENT OF SAFETY AND SECURITY DESIGN CRITERIA

5.1 Prevention through Design

Hazards can be resolved by deciding to either assume the risk associated with the hazard or to eliminate or control the hazard. The Prevention through Design principle, as identified in ANZI Z590.3-2011 *Prevention through Design*, incorporates safety and security considerations into the early design of a system element so as to avoid, eliminate, or mitigate hazard risk to a level as low as reasonably practicable. The following order of precedence shall be applied when incorporating safety considerations into design:

1. Avoidance: Develop concepts of operations, basis of design, or general system requirements to avoid the introduction of hazards to the system.
2. Elimination. Design, redesign or retrofit to eliminate (i.e., design out) the hazards through design selection. This strategy generally applies to acquisition of new equipment or expansion of existing systems; however, it can also be applied to any change in equipment or individual subsystems.
3. Substitution for Minimum Risk. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level. This may be accomplished, for example, through the use of fail-safe devices and principles in design, the incorporation of high-reliability systems and components and use of redundancy in hardware and software design.
4. Engineering Controls. Hazards that cannot be eliminated or controlled through design selection will be controlled to an acceptable level through the use of fixed, automatic or other protective safety design features or devices. This could result in the hazards being reduced to an acceptable risk level. Safety devices may be part of the system, subsystem or equipment. Examples of safety devices include interlock switches, protective enclosures and safety pins. Care must be taken to ascertain that the operation of the safety device reduces the loss or risk and does not introduce an additional hazard. Safety devices will also permit the system to continue to operate in a limited manner. Provisions will be made for periodic functional checks of safety devices.
5. Provide Warning Devices. When neither design nor safety devices can effectively eliminate nor will control an identified hazard, devices shall be used to detect the hazardous condition and generate an adequate warning signal to provide for personnel remedial action. Warning signals and their application will be designed to minimize the probability of incorrect personnel reaction to the signals and will be standardized within like types of systems. Warning signals and their application should also be designed to minimize the likelihood of false alarms that could lead to creation of secondary hazardous conditions.
6. Administrative Controls. Where it is not possible to eliminate or adequately control a hazard through design selection or use of safety and warning devices, procedures and training will be used to control the hazard. Special equipment operating procedures can be implemented to reduce the probability of a hazardous event and a training program can be conducted. The level of training required will be based on the complexity of the task and minimum trainee qualifications contained in training requirements specified for the subject system element and subsystem. Precautionary notations in manuals will be standardized. Safety critical tasks, duties and activities related to the system element and subsystem will require certification of personnel proficiency. However, without specific written approval, no warning, caution or other form of written advisory will be used as the only risk reduction method for unacceptable and undesirable hazards.
7. Personal Protective Equipment and Guards: Where no other higher-level alternative mitigations are possible, the use of personal protective equipment or the installation of guards will be used to mitigate the hazard. Personal protective equipment and guards may be used to supplement other higher-level mitigations, but when they are the only mitigation applied they are to be used only when no other alternatives exist.

5.2 Design Criteria

Design criteria are developed from the engineering experience of the design team obtained from numerous other rail projects, as well as the following sources:

- Formal hazard analyses, including Preliminary Hazard Analysis;
- Threat and Vulnerability Assessments;
- Federal Railroad Administration regulations found in Code of Federal Regulations Title 49, Parts 200-299;
- California Public Utilities Commission (CPUC) General Orders;
- California Building Code;
- California State Fire Marshal's Office direction and recommendations;
- Local building codes and Fire Marshal recommendations;
- National Fire Protection Association (NFPA);
- American Public Transportation Association (APTA);
- American Railway Engineering and Maintenance-of-Way Association (AREMA);
- Underwriters Laboratories (UL);
- Safety and security recommendations of the Department of Homeland Security (DHS), Transportation Security Administration (TSA), and the Federal Transit Administration (FTA);
- Other industry or technical standards.

CHSTS will conduct Preliminary Hazard Analysis and Threat and Vulnerability Assessment during the Preliminary Engineering phase to aid in defining safety and security design criteria.

Design criteria are developed to address system safety and security requirements applicable to the entire system. System safety and security requirements for each specific design element will be incorporated into a Design Manual chapter entitled *CHSTS Design Criteria* with reference to corresponding design criteria for specific engineering elements (e.g., clearances, structures, seismic criteria, etc.).

The processes described in the *CHSTS Verification and Validation Management Plan* (VVMP) will ensure that the design criteria and the basis of design report will incorporate safety and security requirements into the system design.

The following documents have been prepared by the PMT in order to achieve the system's design criteria's objectives:

- Basis of Design Report;
- Risk Management Plan and Hazard Log;
- System Requirements;
- Infrastructure Maintenance Plan;
- Design Manual;
- Standard Drawings;
- Standard Specifications.

A consistent approach will be utilized within all the engineering efforts and will assist the CHSTS Regional Consultant Teams in preparation of their designs.

The *Basis of Design Report* defines the key CHSTS performance requirements. This document serves as the guiding force in establishing the design criteria and development of design standards. The key audience for the Basis of Design Report is the Authority, the Program Manager, the Regional Project Managers, and the Section Designers. The purpose of the report is to guide the Engineering Management Team during the development of engineering criteria and provide the required performance levels for the CHSTS.

A *Risk Management Plan and Hazard Log* will be developed outlining methodologies to ensure that a consistent approach to risk assessment and cost are applied throughout the CHSTS. The plan will address both system safety risk and project delivery risk, and include a Program level risk register that will be regularly updated and maintained.

The *CHSTS System Requirements* provides a common platform for which similar Code of Federal Regulations, CPUC General Orders, and European Union Technical Specifications for Interoperability, as well as other industry best practice and standards, can be collectively presented and assessed at a detailed technical level. In addition to guiding and supporting specific technical guidance at the subsystem level, the CHSTS System Requirements structure is used to demonstrate how the performance objectives of the CHSTS are to be achieved.

The *Infrastructure Maintenance Plan* is a base document outlining how the CHSTS will be maintained. This document sets forth the requirements for maintenance facilities for rolling stock and the railway infrastructure, as well as the approximate location and size of supporting facilities.

Design Criteria have been prepared that is intended to serve as the design requirements for a possible Design/Build consortium. The Design Criteria identifies and specifies required elements and considerations to ensure a safe and reliable operating railway for the CHSTS. The Design Criteria will be supported by *Standard Drawings* and *Standard Specifications* as required.

5.3 Design Reviews

CHSTS drawings and specifications will be reviewed informally during development and formally during preliminary and final design. The purpose of these reviews will be to verify conformance with all of the projects design criteria. These reviews are performed by the corresponding PMT discipline design personnel, their design supervisors, applicable oversight agencies, representatives from the Regional Consultants, and the PMT System Safety and Security staff.

Design reviews will be scheduled and coordinated so as to permit ample opportunity for comments and approvals. After satisfactory resolution of comments, the specifications are “sealed” by professional engineers from the Regional Consultants design group and issued for use.

5.4 Deviations and Changes

For any instances that arise requiring a possible deviation from the safety-critical or security critical design criteria (i.e., physical constraints identified within the system’s corridor conflicting with baseline requirements), the PMT and the associated segment Regional Consultant during Preliminary Engineering (and PMT and design/build contractor during Final Design) will be required to explore all reasonable alternatives to provide a design that conforms to the requirements of the existing criteria. If a reasonable alternative cannot be developed, the requesting party will submit a Design Variance Request (DVR) to the SSPC, whose members include safety and security personnel and representatives of the required engineering disciplines. The requesting party will be responsible for identifying and resolving any hazards or vulnerabilities related to any deviations.

Any deviations to the Design Criteria developed by the PMT or design/build contractors will require a safety and security assessment for each deviation to ensure that the same level of safety and security is achieved as would have occurred had the Design Criteria been followed. A formal hazard analysis and/or TVA may be required to support the safety and security assessment of Design Criteria deviations. If the change request is approved, the findings and recommendations will be incorporated into the Final Design

engineering and construction plans and the Final Design Verification Checklist(s) will be updated to reflect the change.

During the life cycle of the project, the SSPC may also confront design issues that require additional hazard analysis or vulnerabilities assessment, the outcome of which may result in requests for design changes. Such requests will be submitted to the SSPC for review and processed through the Design Variance Request process.

The PMT is responsible for monitoring all design requests/changes for compliance with the Design Criteria or Design Standards documents, including statutory and regulatory requirements and requirements specified in any contract.

6.0 QUALIFIED OPERATIONS AND MAINTENANCE PERSONNEL

6.1 Operations and Maintenance Requirements

The Authority's Operations and Maintenance Team (OMT) will be responsible for developing system operations and maintenance requirements that support the safe and efficient operation of the California High-Speed Train system. Principal activities of the OMT include the following:

- Provide ongoing operations input to the Engineering Management Team and Regional Engineering teams in the development of system design elements
- Review and comment on engineering design elements to ensure responsiveness to operations' functional requirements
- Coordinate with FRA on development of CHSTS rules and procedures and their relationship to current regulations and new regulations that will emerge from the CHSTS. Key categories include:
    - Code of Federal Regulations (CFR) regulatory issues
    - Rail System Operating Rules
    - System Safety Rules and Procedures
    - Standard Operating Procedures
    - Emergency Action Plans and Procedures
- Coordinate with railroads, operating agencies/rail service providers and stakeholders as required

Personnel staffing requirements for the operation and maintenance of the in-service CHSTS will be established and described in the *CHSTS Training and Personnel Qualification Plan*, to be developed prior to the startup of revenue operations.

Development of the *CHSTS Operations and Maintenance Plan* for any system or subsystem component will begin during Construction Phase. Position titles, responsibilities, qualifications, and training requirements will be identified consistent with other high-speed rail operating systems using similar technologies and operating characteristics. The magnitude of the in-service CHSTS (trains operated, vehicles in service, track and OCS systems to maintain) will determine staffing levels for operators, maintainers, and supervisors.

Additionally, the *CHSTS Infrastructure Maintenance Requirements Plan* (IMRP) establishes and describes how infrastructure maintenance will be planned and implemented including methods utilized and resources required. The IMRP specifies the CHSTS requirements necessary to meet passenger and public safety levels that meet or exceed FRA Class 6 Regulatory Safety Standards, consistent with FRA's High-Speed Passenger Rail Safety Strategy. IMRP requirements will be incorporated into the system Design Criteria during the Preliminary Engineering phase of the CHSTS.

6.2 Operations and Maintenance Plans, Rules and Procedures

The following documents will be revised for the CHSTS during the Project Construction Phase, in preparation for Testing and Startup:

- Concept of Operations
- Code of Operating Rules
- Rolling Stock Maintenance Plan
- Infrastructure Maintenance Requirements Plan
- Training and Personnel Qualification Plan
- Service/Operating Plan
- Command and Control Facilities Plan
- On-Board Operating Plan
- Passenger Station Operating Plan
- Passenger Train Emergency Preparedness Plan
- Air Brake Operating Instructions
- Electrical Operating Instructions
- Emergency Operating Procedures
- Timetable Special Instructions
- On-Track Safety Rules
- System Safety Program Plan
- System Security Plan
- Security and Emergency Preparedness Plan

6.3 Training Program

The Authority will be responsible for ensuring qualified O&M personnel assigned to the CHSTS are trained to perform pre-revenue and revenue operations. Instruction in safe methods of operation, safety requirements, security awareness and emergency response procedures will be included in manuals, handbooks, and other documentation developed for the training and certification of operations and maintenance personnel. Training plans, which include in-house classroom training and on-the-job training and testing, will be developed based on the individual characteristics of the equipment or CHSTS locations.

The future CHSTS Operators, Instructors and Field Supervisors will undergo familiarization training on all operational equipment, rules, plans and procedures. The future Central Control Operations Staff (including Superintendents, Supervisors, and Train Dispatchers) will require extensive training and qualification on the train control system, in addition to operating rules and procedures, and safety and security procedures.

Positions which will require detailed job descriptions and training programs prior to entering the Testing Phase of the CHSTS include, but are not limited to the following:

- Superintendents
- Operations Supervisors
- Train and Engine Service Employees
- Control Center Supervisors
- Control Center Train Dispatchers
- Equipment Maintenance Employees
- Signal and Communications Employees
- Maintenance of Way Employees
- Power and OCS Employees

Contractors and suppliers providing equipment and facilities for the CHSTS will be responsible for developing training plans, training manuals, and conducting training courses for applicable CHSTS Operations and Maintenance staff. Contractors will be required to develop and implement programs to train appropriate Authority personnel in the operation and maintenance of each piece of equipment or systems provided in conformance with the *CHSTS Training and Personnel Qualification Plan*.

6.4 Emergency Preparedness

A *Passenger Train Emergency Preparedness Plan* (PTEPP) will be developed prior to the start of the Testing Phase of the CHSTS to prepare for emergency incidents that may occur during testing. The PTEPP will be further developed and carried over into the start of revenue service. The PTEPP will contain emergency preparedness requirements and procedures for the Operations and Equipment Maintenance disciplines, in compliance with 49 CFR, Part 239. The PTEPP will identify requirements for a program of training (including instructional programs, emergency preparedness drills and tabletop exercises) of railroad operating and maintenance personnel and emergency responders. The goal of the PTEPP is to verify and validate the following:

- Adequacy of emergency plans and procedures
- Readiness of railroad operating and maintenance personnel to perform under emergency conditions
- Effective coordination between railroad operations and emergency response agencies – police, fire, and emergency medical services
- Familiarization of fire, police, and emergency medical services personnel with the physical and operating characteristics of CHSTS operations and inherent hazards

After-action reviews will be conducted following any major emergency response event or exercise prior to the start of revenue operations. A report of the findings will be provided to the SSPC. Action items will be tracked by the SSPC to completion through the V&V process. Outcomes may include recommendations for revisions to the PTEPP, operating rules or procedures, equipment or infrastructure changes, or emergency responder procedures, and changes to training plans and training programs pertaining to emergency response and personnel.

Fire/Life Safety and Security Committees will be established at both a regional and State level as described in Section 3.3.3 of this SSMP to provide a vehicle for clear, consistent communication with emergency responders.

7.0 SAFETY AND SECURITY CERTIFICATION PROGRAM

7.1 Overview

The California High-Speed Rail Authority is ultimately responsible for ensuring that all safety-critical and security-critical elements of the CHSTS are designed, constructed, tested, and made operationally ready in a safe and secure manner prior to the start of revenue service. The Safety and Security Certification Program describes the responsibilities and processes required to demonstrate that the CHSTS is safe and secure, in conformance to the FTA *Handbook for Transit Safety and Security Certification* and Federal Railroad Administration (FRA) Regulations 49 CFR 236, Sub-parts H and I for Positive Train Control, and other FRA Regulations as applicable. The Safety and Security Certification Program applies to all phases of the CHSTS, from preliminary engineering to the start of revenue operations, for each segment designed and built for the system.

The Safety and Security Certification Program (SSCP) is comprised of verification and validation processes and principles consistent with the program-level *Verification and Validation Management Plan* (VVMP). The SSCP scope encompasses safety and security certification of the facilities, systems and equipment, safety-related procedures, training programs, and hazard and vulnerability resolution activities and operational readiness for the project. The process can be categorized into distinct progress factors throughout the advancement of the project. Specifically, safety and security certification focuses on the following certifiable factors:

- Design Criteria Conformance
- Construction Specification Conformance
- Safety-Related Testing Conformance
- Hazard and Vulnerability Resolution Conformance
- Operations and Maintenance Manuals Conformance
- Rules and Procedures Conformance
- Training Conformance
- Emergency Drills Conformance
- Integration Testing and Start-up.

Certification will be performed by contract once the Project moves beyond the PE Phase. Certification of latter-phase contracts may consist of one or more certifiable elements defined in Section 7.4.1 and may include all or a few certifiable factors. The exceptions to this are the system wide activities such as procedures, training, emergency drills and integration testing and start-up which will be certified for the complete system.

After completion of each certifiable factor a Certificate of Conformance (COC) is issued. The COC required for the various components necessitate the performance of a variety of system safety, security, and fire/life safety activities. The activities may be performed either independently, or integrated with other tasks such as acceptance testing or quality control measures. Regardless of whether the activities are performed independently or integrated with others, adequate system safety, security, and fire / life safety activity records must be developed and maintained as evidentiary support for the COC.

The verification and validation (V&V) process defined in VVMP will be used to implement and monitor the certification process. Generally safety V&V methodology is comprised of conformance with the design criteria and collection of drawings, analyses, tests, calculations, observation, measurements, etc., performed at different stages in system development to demonstrate compliance with all safety requirements. Verification and Validation activities involve a number of analyses such as hazard analyses, operational analysis, and risk analyses; data collection; performance evaluation; field measurements; and product refinement including subsystem testing, field testing, integration testing and revenue service testing.

The Authority Risk Manager, with the assistance of the PMT Safety Manager and PMT Security Manager, will have overall responsibility for the administration of the Safety and Security Certification Program. The PMT Safety Manager, in coordination with and in conjunction with the PMT Operations Manager and

Engineering Manager will be responsible for initiating the safety and security certification process during the preliminary engineering phase of the CHST Project. The PMT led by the PMT Safety Manager, will develop a *Certifiable Elements and Hazards Log* (CEHL) for safety-critical and security-critical system elements and their associated hazards and the mitigations developed during the hazard analysis process. The CEHL will carry though all of the project phases to ensure that hazards identified in the Preliminary Engineering Phase are mitigated consistently throughout the project life cycle.

Mitigations will provide input to the design criteria in the form of requirements. The design criteria will then be examined for all safety-critical items that must be certified, resulting in Certifiable Items Lists that include all mitigations from the hazard analysis plus other identified safety-critical items. Certifiable Items Lists for each project phase lead in turn to development of Certifiable Items Lists for the subsequent project phase.

Certifiable Items Lists that are specific to safety and security requirements will be distinctly identified as such and tracked in conformance with the VVMP, and collectively make up the verification and validation evidence that supports safety and security certification.

7.2 Program Goals and Objectives

The goals of the Safety and Security Certification Program are to verify that identified safety and security requirements have been met in the preliminary engineering, final design, and construction phases and to provide evidence that the CHSTS is safe and secure for revenue service. The objectives of the Safety and Security Certification Program are to document the following:

- Safety and security design criteria are reflected in contract documents
- Facilities and equipment have been designed, constructed, manufactured, inspected, installed, and tested in accordance with safety and security requirements
- Operations and maintenance procedures and rules have been developed and implemented to ensure safe operations
- Training documents have been developed for the training of operating and emergency response personnel
- Transportation and maintenance personnel have been trained and qualified
- Emergency response agency personnel have been prepared to respond to emergency situations in or along the CHSTS corridor
- Safety and security systems integration tests have been conducted
- All safety and security related issues have been addressed and resolved

Certification occurs at the beginning of each project phase, and is required for advancing system elements into the next phase. For example, the Final Design of a bridge structure must be certified to meet all safety and security design criteria prior to construction, and then must be certified to have been built in conformance to those safety and security design criteria before being placed into operation. This process assures the Authority that CHSTS elements are safe and secure as they move through each successive phase of the System development.

Certification Items that are not completed prior to moving to the next phase are placed on an Open Items List and tracked to completion. The Open Items List describes a plan for closure of the Certifiable Items, including target dates and an accountable person for closure.

7.3 Responsibilities

Safety and security certification is managed by the Authority Risk Manager through the oversight and participation of the SSPC, and with the ultimate approval of the Authority through the SSEC.

The SSPC will be responsible for tracking the progress of safety and security certification through regular review and update of Hazard and Threat and Vulnerability Logs maintained by the PMT Safety Manager and PMT Security Manager.

Federal Railroad Administration approval to operate will be achieved through final safety and security certification prior to the start of revenue service.

7.4 Safety and Security Certification Process

The CHSTS safety and security certification process will follow the methodology defined in detail in VVMP. The certification process will be divided in the following distinct stages and steps.

- Stage 1: Environmental Review / Preliminary Engineering
- Stage 2: Design / Build Contracts
    a) Step 1: Final Design
    b) Step 2: Construction
    c) Step 3: Testing / Acceptance
- Stage 3: Final Integration, Testing and Certification

During the preliminary engineering phase Preliminary Hazard Analysis (PHA), Site-specific Hazard Analysis (SiSHA) and Threat and Vulnerability Assessment (TVA) will be performed. Hazards are identified by various means such as historical data, generic hazard checklists, conceptual design, already developed design criteria, scenario development and the subjective judgment of a hazard management team during formal brainstorming workshop sessions. The hazard analysis is then performed on the identified hazards. The principal means of identifying security-related design criteria are Threat and Vulnerability Assessments (TVA) conducted by the PMT Security Manager in collaboration with the other PMT discipline technical experts. Other analyses are conducted as necessary. The adopted mitigation measures from the PHA and TVA could provide input to design criteria or can be tracked on the CEHL and CETVL. The mitigation measures identified in SiSHA are contract specific and are tracked for resolution in the specific Design/Build (D/B)contract.

Each D/B contract will be certified in three steps as defined in VVMP. Once all design/build contracts have been successfully completed and certified, the CHSTS as a whole system will be integrated, tested and certified under supervision of the Authority.

7.4.1 Certifiable Elements

The Project has defined eight major CHSTS components for safety and security certification. They are referred to as the “Certifiable Elements”. Some or all of the eight certifiable factors defined in Section 7.1 will apply to each of the following eight “Certifiable Elements”. Samples of sub-elements are listed under the Certifiable Elements. The sub-element listing will be modified and expanded as the safety and security certification requirements are developed in the requirement management tool of SSMP.

A Trainway
   a. Track
   b. Structures
   c. Tunnel
   d. Alignment
   e. Access/egress facilities

B Station(s)
   a. Escalators
   b. Elevators
   c. Station structure
   d. Stand-by generators
   e. Platform
   f. Concourse

C Support Facilities
   a. Storage/setup Yards
   b. Vehicle Maintenance Facilities
   c. Track maintenance facilities
   d. Operations Control Center

D Traction Power
   a. Traction Power Substations
   b. Switching Stations
   c. OCS

E Ventilation
   a. Emergency Ventilation System
   b. Ventilation Structure

F Train Control
   a. Automatic Train Protection

G Communications
   a. Radio
   b. Closed Circuit TV
   c. Emergency Telephone
   d. Emergency Trip Station
   e. Fire Telephone
   f. Public Address System

H Utilities
   a. HST Power Facilities
   b. HST Fuel Lines
   c. HST Water/Sewer
   d. HST Communications
   e. Non-HST Power
   f. Non-HST HazMat Pipes
   g. Non-HST Carrier Pipes non-HazMat
   h. Non-HST Water/Sewer

7.4.2 Tracking of Hazards and Vulnerabilities

A *Certifiable Elements and Hazards Log* will be established during the Preliminary Engineering Phase. The CEHL identifies the major elements of the CHSTS that are to be proven to be safe prior to the startup of revenue service and acts as a guide for the certification process throughout project life cycle. Hazards associated with each major element that can reasonably be expected to occur in the CHSTS will be identified through a Hazard Analysis process and placed on the CEHL. The CEHL will be developed by the PMT System Safety Manager in collaboration with the other PMT discipline technical experts and presented to the SSPC for review and approval. The CEHL will be updated and expanded following the completion of analyses during the various phases of the CHSTS. A sample CEHL is shown in Figure 7-1. Regular updates of the log will be presented to the SSPC and included in the quarterly reports to the SSEC.

For security certification a *Certifiable Elements and Threats and Vulnerabilities Log* (CETVL) will be established during the Preliminary Engineering Phase. The CETVL identifies the major elements of the CHSTS that are to be proven to be secure prior to the startup of revenue service and acts as a guide for the certification process throughout project life cycle. The CETVL will be developed by the PMT System Security Manager in collaboration with the other PMT discipline technical experts and presented to the SSPC for review and approval. The CETVL will be updated and expanded following the completion of security analyses during the various phases of the CHSTS. The CETVL format will be similar to CEHL.

Figure 7-1 CEHL (Sample)

California High-Speed Train System
Certifiable Elements and Hazards Log

Certifiable Elements			Hazards				Mitigations		
No.	System Elements	Sub-Elements	No.	Date Identified	Site Specific	Description	Mitigation Description	Notes/Comments	PE Phase Reference
1.1	R-O-W Generally								
1.1.1	R-O-W Generally	Derailment	1.1.1.1	8/30/2011	No	Track Failure - Cracked or broken track component	1) O&M program and remedial maintenance methodology that meet or exceed FRA Guidelines for Track Class to operate at 220 MPH (when developed).		
							2) Track component quality standards that meet or exceed AREMA requirements.		
							3) Install on-board derailment containment devices.		
							4) Install in-track derailment containment elements.		
							5) Require positive indication of broken rail through track circuit system.		
			1.1.1.2	8/30/2011	No	Track Abnormality - Worn track components, cross-level	1) O&M program and remedial maintenance methodology that meet or exceed FRA Guidelines for Track Class to operate at 220 MPH (when developed).		
							2) Track component quality standards that meet or exceed AREMA requirements.		
							3) Install on-board derailment containment devices.		
							4) Install in-track derailment containment elements.		
							5) Require positive indication of broken rail through track circuit system.		
			1.1.1.3	8/30/2011	No	Roadbed failure due to subsidence, shifting ground, etc.	1) Perform geotechnical analysis and incorporate results into sub-grade design.		
							2) Install appropriate drainage.		
							3) Inspection and maintenance of drainage systems.		
			1.1.1.4	8/30/2011	Yes	Washout caused by flooding or scouring	1) Perform hydraulics analysis and incorporate results into sub-grade design, slope protection and setting of profile.		
							2) Install scour protection (revetment or other structure) to protect sub-grade from water course.		
							3) Install culvert or bridge structure where crossing water course.		
			1.1.1.5	8/30/2011	Yes	Slide caused by hillside movement, storm water runoff	1) Perform geotechnical analysis to evaluate slope stability that could effect the HSR trackway.		
							2) Perform hydraulics analysis and incorporate results into sub-grade design, slope protection and setting of profile.		
							3) Inspection and maintenance of drainage systems.		
							4) Identification and monitoring of potential hazardous locations.		
			1.1.1.6	8/30/2011	Yes	Seismic activity	1) Perform seismic analysis to determine potential limits of ground movement at the location.		
							2) Mitigate the effects of seismically-induced forces and deformations due to ground motions resulting from an	Wording revised 1/25/13 during review of DC Chapter 11.	
							3) Install earthquake monitoring devices at regular intervals for notification of seismic event.		
							4) Establish an operational response based upon notification of a seismic event.		
							5) Identification and monitoring of potential hazardous locations.		
			1.1.1.7	8/30/2011	Yes	High winds	1) Perform wind analysis for effects on vehicles and operations.		
							2) Install weather stations at regular intervals to monitor wind conditions.		
							3) Develop operational responses to extreme wind conditions.		
							4) Install wind barriers at high-risk locations where need is supported by wind analysis.		
			1.1.1.8	8/30/2011	Yes	Buildup of snow or ice	1) Develop site-specific snow/ice analysis for Tehachapi Pass.		
							2) Employ widened roadbed to avoid buildup of snow drifts.	Per EMT/Harris 11/27/12, this mitigation will not be employed.	
							3) Intall switch heaters at locations of anticipated snow/ice buildup.	Per EMT/Harris 11/27/12, this mitigation will not be employed.	
							4) Develop O&M practices for mitigation of snow/ice buildup.		
1.1.2	R-O-W Generally	Collision	1.1.2.1	8/30/2011	No	Collision between HSR trains	1) Track center spacing exceeds the combined dynamic envelopes of the trains.	Wording revised per EMT/Harris 11/27/12.	
							2) ATC prevents collision between trains as a core functional requirement.		

Note – Figure 7-1 is a sample representation only. Refer to current CEHL for identified hazards and required mitigations. Due to space considerations Figure 7-1 only depicts Preliminary Engineering and Final Design phases; subsequent phases will be added as the project matures.

7.4.3 Certifiable Items Lists

The Design Criteria Manual establishes criteria, guidelines and requirements for the design of Infrastructure and Systems elements of the CHSTS. These criteria include design survey and mapping, trackway clearances, track geometry, trackwork, rolling stock and vehicle intrusion protection, civil, drainage, utilities, geotechnical, seismic, structures, tunnels, stations, support facilities, facility power and lighting systems, traction power supply systems, overhead contact system and traction power return

system, grounding and bonding requirements, corrosion control, automatic train control, yard signaling, electromagnetic compatibility and interface, supervisory control and data acquisition subsystems, communications, rolling stock–core systems interfaces and, safety and security. The design criteria shall be reviewed by the PMT System Safety Manager for safety-critical items that must be certified, whether or not they were developed as a result of the hazard analysis activities. All safety-critical items will be added to a Certifiable Items List and verified in conformance with the V&V process identified in the VVMP. The tool for tracking V&V compliance is the Certifiable Items List. A sample Certifiable Items List is shown in Figure 7-2.

Figure 7-2 Certifiable Items List (Sample)

CHSTS SAFETY & SECURITY CERTIFICATION PROGRAM
CERTIFIABLE ITEMS LIST

Item # _____ Item Description _____

Project Phase _____ Developed By _____ (Name) _____ (Date)

Sub-Item #	Description	Criteria	Verification Date	Verification Initials	Objective Evidence/ Means of Verification
1					
2					
3					
4					
5					
6					
7					
8					
Comments / Restrictions					

Safety Manager Review _____ (Manager) _____ (Date)

SSPC Review _____ (Chairman) _____ (Date)

SSEC Review _____ (Chairman) _____ (Date)

SAMPLE

V&V Certifiable Items Lists for each project phase lead in turn to development of V&V Certifiable Items Lists for the subsequent project phase.

7.4.4 Verification and Validation of Final Design and Construction

Design Criteria are requirements for the Final Design. The verification and validation process, as identified in the *CHSTS Verification and Validation Management Plan*, will be utilized for verifying that the identified mitigations have been satisfactorily incorporated into the Final Design.

The Design/Build Contractors will be responsible for completing the Certifiable Items Lists applicable to their specific project scope during the Final Design Phase. The Design/Build Contractors will identify in the resolution section of the Certifiable Items Lists objective evidence that demonstrates compliance with the required safety-critical or security-critical design criteria. Requests for variance from the requirements identified in the Certifiable Items Lists will be handled through the process identified in Section 5.4.

All completed Certifiable Items Lists, along with associated supporting material, will be compiled by the Design/Build Contractors and available for audit by the PMT System Safety Manager upon request. When all Certifiable Items Lists for a particular element or infrastructure component are completed, a Final

Design Certificate of Conformance Package consisting of a Certificate of Conformance for the project element, all completed Certifiable Items Lists, and all supporting documentation such as hazard analysis, drawings, and design element descriptions will be compiled.

The Certifiable Items Lists will be expanded by the Design/Build Contractors to include a Construction section upon completion of the Final Design phase of a particular CHSTS element. The safety- and security-critical items identified during the Final Design Phase will be carried over into the Construction Phase.

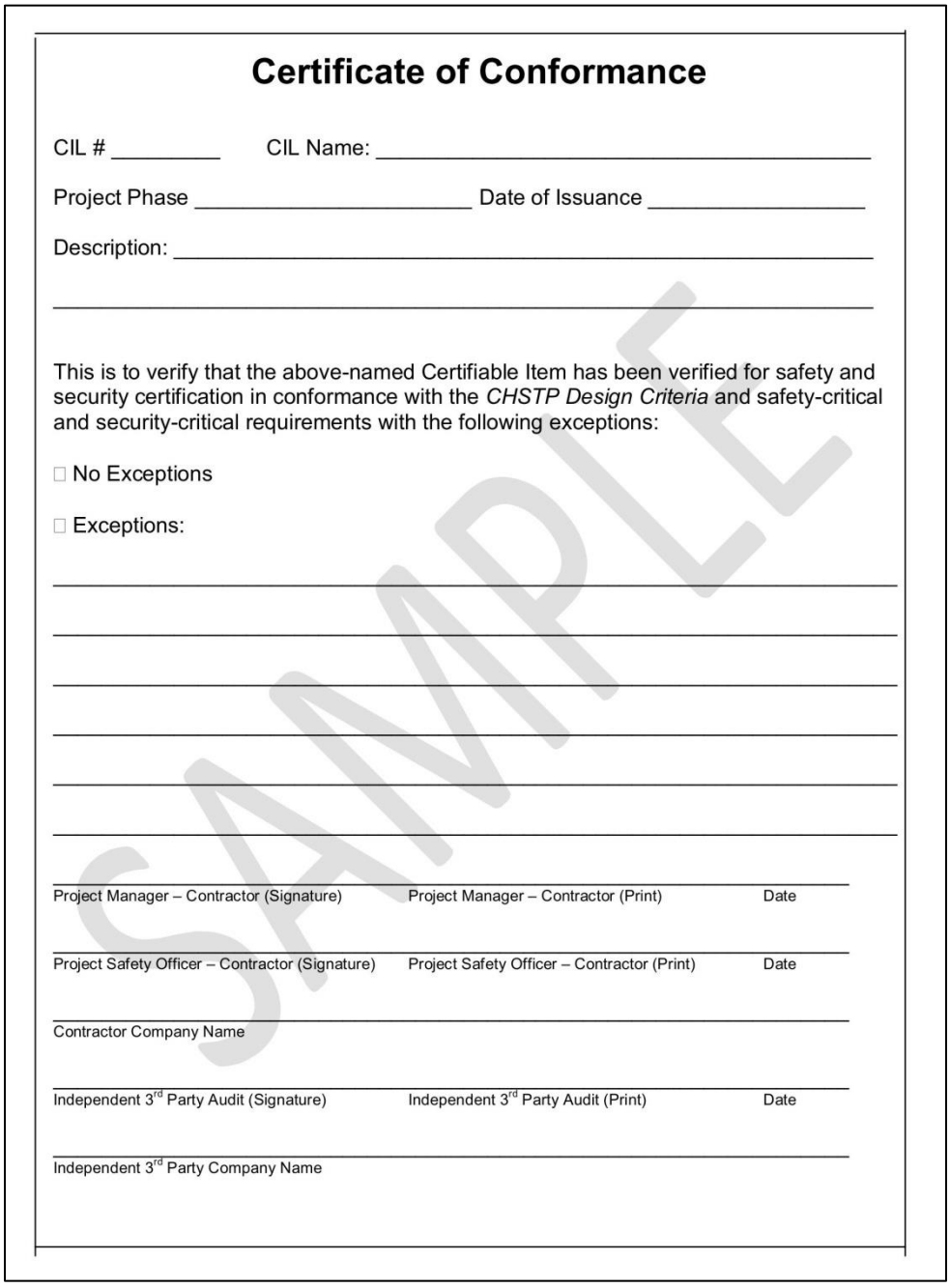
The Design/Build Contractors will be responsible for completing the Certifiable Items Lists that apply to their scope of work during the Construction Phase. The Design/Build Contractors shall identify in the resolution section of the Certifiable Items Lists objective evidence that demonstrates compliance with design features that are identified as safety-critical or security-critical. Requests for variance from the requirements identified in the Certifiable Items Lists will be handled through the process identified in Section 5.4.

All completed Certifiable Items Lists, along with associated supporting material, will be compiled by the design/build contractors and available for audit by the PMT System Safety Manager upon request. When all Certifiable Items Lists for a particular element or infrastructure component are completed, a Construction Certificate of Conformance Package consisting of a Certificate of Conformance for the project element, all completed Certifiable Items Lists, and all supporting documentation such as hazard analysis, field reports, photographs, and drawings will be compiled.

All completed Certificate of Conformance Packages (Final Design or Construction) will be submitted to the SSPC for review by the SSPC, and eventual review and acceptance by the Authority through the SSEC.

A sample Certificate of Conformance is shown in Figure 7-3.

Figure 7-3 Certificate of Conformance (Sample)



Certificate of Conformance

CIL # _____ CIL Name: _____

Project Phase _____ Date of Issuance _____

Description: _____

_____

This is to verify that the above-named Certifiable Item has been verified for safety and security certification in conformance with the *CHSTP Design Criteria* and safety-critical and security-critical requirements with the following exceptions:

☐ No Exceptions

☐ Exceptions:

_____

_____

_____

_____

_____

_____

_____
Project Manager – Contractor (Signature) Project Manager – Contractor (Print) Date

_____
Project Safety Officer – Contractor (Signature) Project Safety Officer – Contractor (Print) Date

_____
Contractor Company Name

_____
Independent 3rd Party Audit (Signature) Independent 3rd Party Audit (Print) Date

_____
Independent 3rd Party Company Name

SAMPLE

7.4.5 Testing Verification

The Certifiable Items Lists will be expanded by the PMT System Safety Manager to include a Testing section upon completion of the Final Design phase of a particular CHSTS element. The safety- and security-critical items for systems identified during the Final Design and Construction Phases will be carried over into the Testing Phase. In addition, the relationships between systems and subsystems will be analyzed for systems integration requirements as identified in a Systems Integration Test Plan, and Certifiable Items Lists for integrated testing will be developed to prove the integration of associated systems.

The Systems Contractor(s) will be responsible for any additional analyses that are required (PHA, TVA, FMEA, IHA, SHEA, FTA and OHA as appropriate), as the safety-critical or security-critical testing criteria are developed and applied to specific CHSTS or subsystem elements. The systems contractor(s) will be responsible for developing and completing the Certifiable Items Lists that apply to their scope of work during the Testing Phase. The system(s) contractor must identify in the resolution section of the Certifiable Items Lists objective evidence that demonstrates compliance with testing requirements that are identified as safety-critical or security-critical. Requests for variance from the requirements identified in the Certifiable Items Lists will be handled through the process identified in Section 5.3.

All completed Certifiable Items Lists for system testing or system integration, along with associated supporting material, will be compiled by the systems contractor(s) and available for audit by the PMT System Safety Manager upon request. When all Certifiable Items Lists for a particular system element or integrated system relationship are completed, a Testing Certificate of Conformance Package (consisting of a Certificate of Conformance for the required system tests, all completed Verification Checklists, and all supporting documentation such as hazard analysis, field reports, photographs, and drawings) will be compiled and forwarded to the PMT System Safety Manager. The PMT System Safety Manager will review the Testing Certificate of Conformance Package for completeness and content accuracy, and will then forward the Testing Certificate of Conformance Package to the SSPC for review and acceptance through the issuance of SONO. If accepted by the SSPC, the Testing Certificate of Conformance Package is forwarded to the SSEC for ultimate Authority review, approval and certification.

7.4.6 Startup Verification

The Certifiable Items Lists will be expanded by the PMT System Safety Manager to include a Startup section as the CHSTS is prepared for the start of revenue operations. The safety- and security-critical items for operational readiness of the CHSTS identified during the Final Design, Construction and Testing Phases will be carried over into Startup. Certifiable startup items include but are not limited to operation plans, emergency preparedness plans, training programs, timetables and rulebooks.

The O&M contractor(s) will be responsible for completing the Certifiable Items Lists that apply to their scope of work prior to Startup. The O&M contractor(s) must identify in the resolution section of the Verification Checklists objective evidence that demonstrates compliance with requirements for the start of revenue operations that are identified as safety-critical or security-critical. The O&M contractor(s) will be responsible for any additional analyses that are required (PHA, TVA, FMEA, IHA, SHEA, FTA and OHA as appropriate), as the safety-critical or security-critical criteria for startup are applied to specific CHSTS, subsystem or operational elements. Requests for variance from the requirements identified in the Certifiable Items Lists will be handled through the process identified in Section 5.3.

All completed Certifiable Items Lists for the start of revenue operations, along with associated supporting material, will be compiled by the O&M Contractor(s) and available for audit by the PMT System Safety Manager upon request. When all Certifiable Items Lists for a particular system or operational element are completed, a Startup Certificate of Conformance Package (consisting of a Certificate of Conformance for the startup requirements, all completed Certifiable Items Lists, and all supporting documentation such as hazard analysis, field reports, photographs, and drawings) will be compiled and forwarded to the PMT System Safety Manager. The PMT System Safety Manager will review the Startup Certificate of Conformance Package for completeness and content accuracy, and will then forward the Startup Certificate of Conformance Package to the SSPC for review and acceptance through the issuance of SONO. If accepted by the SSPC, the Startup Certificate of Conformance Package is forwarded to the SSEC for ultimate Authority review, approval and certification.

7.4.7 Open Items List

Certifiable Items that cannot be closed prior to the start of the next project phase shall be placed on an Open Items List for tracking purposes. The Open Items List will describe the Certifiable Item itself, restrictions or conditions that permit the movement of the project element to the next project phase, a target date for closure, and a person of accountability for the certifiable item. The Open Items List will be

maintained by the PMT System Safety Manager and periodically reviewed by the SSPC for progress and completeness.

7.4.8 Conditional Use Permit

Certifiable Items that require placement on the Open Items List will be reviewed by the PMT System Safety Manager and additional hazard analysis applied as appropriate. The results of the hazard analysis will be incorporated into a Conditional Use permit that describe the conditions or restrictions that allow the use or advancement of the certifiable item into the next project phase before certification for that item is complete. The Conditional Use Permit will be presented to the SSPC for review and SONO. The Conditional Use Permit will describe all conditions or restrictions associated with the conditional use of the Certifiable Item, including an expiration date. Revisions to the Conditional Use Permit, including extension of the expiration date, will require further review and SONO by the SSPC.

8.0 CONSTRUCTION SAFETY AND SECURITY

8.1 Overview

The purpose of the construction safety and security program is to define the minimum health, safety and security requirements to which all participating CHSTS staff, contractors and subcontractors shall adhere to in fulfilling the Authority's commitment to ensuring a safe and secure construction project. This commitment includes the prevention of job-related injuries and illnesses for the workers engaged in project construction activities, as well as providing safe and secure conditions during construction of the project for the members of the public, who live, work or travel near to the project work areas.

All applicable codes and regulations must be followed by employees engaged in construction activities, including but not limited to the following:

- California Code of Regulations Title 8 Construction Safety Orders
- Federal Railroad Administration regulations as found at 49 CFR 214, 49 CFR 219, 49CFR225, 49 CFR 228, 49 CFR 236
- CPUC General Orders
- Other applicable federal and state OSHA regulations

Contractors will be required to develop a Site-Specific Health and Safety Plan (SSHASP) and a Site-Specific Security Plan (SSSP) that identifies the local conditions and requirements peculiar to the site and work to be performed, and is in compliance with the above regulations.

Contractors are responsible for ensuring the compliance of their employees and subcontractor's with the SSHASP and SSSP.

8.2 Program Elements

The *CHSTS Construction Safety and Security Program* (Appendix B) describes the basic programmatic requirements for construction safety and security, compliance to which is required through the CHSTS construction contract documents. Basic elements of the construction Safety and Security Program include Site-Specific Health and Safety Plans, which are described below.

8.2.1 Site-Specific Health and Safety Plans

The Construction Contractor will be responsible for all aspects of safety and security at the project work site, as required through the standard contract provisions. The Construction Contractor will be required to develop and implement a SSHASP specific to its contract work on the CHSTS, in conformance with the *CHSTS Construction Safety and Security Program*. A site-specific Job Hazard Assessment (JHA) will be performed by the Contractor to determine the safety processes, equipment utilized, and personnel assignments to be provided by the Contractor at each project work site.

The SSHASP will provide details on how the contractor will fulfill the contract safety and security requirements, and will be submitted to the PMT for review and approval.

8.2.2 Construction Safety and Security Management

The construction contractor will be responsible for developing and implementing a Site-Specific Health and Safety Plan and Site-Specific Security Plan in conformance with the requirements of the *CHSTS Construction Safety and Security Program*. The construction contractors will also be responsible for demonstrating self-certification of safety-critical and security-critical certifiable items as identified through the CHSTS V&V process and documented in the V&V Requirements Management Tool database.

The CHSTS Construction Manager will be responsible for the management oversight of the entire construction safety and security program. The CHSTS Construction Management staff will verify contractor compliance with the safety and security requirements of the approved SSHASP and other safety/security related contract provisions, and applicable regulations throughout the construction, testing

and start-up phases of the CHSTS. The CHSTS Construction Management staff will audit construction contractor submissions involving safety and security designs, testing, construction activities and V&V Conformance Checklists. Results will be reported to the Safety and Security Project Committee in compliance with the CHSTS Safety and Security Certification Program described in Section 7.0.

8.2.3 Stop Work Order

The CHSTS construction management plan will establish procedures regarding control of nonconforming work and stop work orders. In the event that a failure to meet safety and/or security requirements results in imminent danger to workers or the general public or property, a Stop Work Order will be issued by the CHSTS Construction Manager.

The CHSTS stop-work procedure shall apply to all construction activities. The stop-work procedure will be used only where imminent danger situations exist. An "imminent danger" is any condition or practice that could reasonably be expected to cause death or serious physical harm immediately or before the danger can be eliminated by normal means.

Stop-work orders will be in effect until the issuing authority determines that the problem(s) is resolved and the work area(s) is brought to satisfactory conformance with health, safety and security requirements.

8.3 Construction Phase Hazard and Vulnerability Analysis

The CHSTS is committed to identifying and managing construction safety hazards and security vulnerabilities as subdivisions within the general issue of project risk. Risk in this context includes those events that, if they do occur, could impact safety, security, the environment, CHSP System's interests or the interests of third parties, including property owners and municipalities.

8.3.1 Risk Management

Risk Management is utilized by the CHSTS as a decision support tool, specifically identifying areas of high risks, which are reviewed to ensure that all reasonable practicable measures are taken to mitigate them. Risk Control measures shall be identified for all risks to the System. These include financial and schedule risks as well as property, safety and security risks.

For the construction phase, prior to finalization of the contract documents, surveys to identify any unique hazards, threats, or vulnerabilities that may exist for the particular construction elements will be conducted and actions to mitigate these hazards or vulnerabilities will be included in the Special Provisions of the specific contract package.

During construction, each contractor shall cooperate with CHSTS staff and other interested parties in providing information needed in connection with risk management of its contract works. The contractor will prepare and submit to the PMT Risk Manager a Risk Management Plan for review and acceptance. The Risk Management Plan shall be based upon the CHSTS *Program Risk Management Plan* and shall include a means of monitoring progress in the reduction of the overall number and impact of risks through the use of a Risk Register which shall be in a format acceptable to the PMT Risk Manager. Safety hazards and security vulnerabilities shall be identified as risks, and will be included as special categories in the Risk Register.

During the contract each contractor's Risk Register shall be updated monthly and submitted to the PMT in hard copy and electronic formats. The risks identified by the contractor shall be integrated into the CHSTS Risk Register.

The Contractor's Risk Management process shall ensure that as far as is reasonably practicable:

- All risks are identified;
- Judgments are made as to risk importance;
- Risk exposure is reduced to acceptable levels;
- Risk control measures are assessed against cost benefit as appropriate; and

- Control measures are reviewed and managed until close out.

For the top “critical” risks from the Risk Register each contractor shall provide a narrative for each Critical risk identified in this category section and the mitigation plan proposed. Safety hazards and security vulnerabilities will be treated as separate categories of risk, and will be classified as Critical depending on specific site conditions.

9.0 STATE SAFETY OVERSIGHT REGULATIONS

9.1 Applicability

The California High-Speed Train System does not fall under the Federal Transit Administration applicability regulations for State Safety Oversight, described in 49 CFR 659. As such, this section does not apply. The Federal Railroad Administration has authority for oversight of safety regulations.

10.0 COORDINATION WITH FEDERAL RAILROAD ADMINISTRATION

10.1 Activities

The California High-Speed Train System will design and construct a railroad system that is regulated by the Federal Railroad Administration. FRA regulation is by directive under the United States Department of Transportation.

Effective on the date the Railroad begins revenue operations, the following generally applicable federal railroad safety regulations from Title 49, Code of Federal Regulations, and any amendments thereto are made applicable to the CHSTS, except where the CHSTS is granted relief through an FRA waiver.

- Part 207, Railroad Police Officers
- Part 209, Railroad Safety Enforcement Procedures
- Part 210, Railroad Noise Emission Compliance Regulations
- Part 211, Rules of Practice
- Part 212, State Safety Participation Regulations
- Part 213, Track Safety Standards
- Part 214, Railroad Workplace Safety
- Part 215, Freight Car Safety Standards
- Part 216, Special Notice and Emergency Order Procedures
- Part 217, Railroad Operating Rules
- Part 218, Railroad Operating Practices
- Part 219, Control of Alcohol and Drug Use
- Part 220, Railroad Communications
- Part 221, Rear End Marking Device
- Part 222, Use of Locomotive Horns at Public highway-Rail Grade Crossings
- Part 225, Railroad Accidents / Incidents: Reports, Classification and Investigations
- Part 227, Occupational Noise Exposure
- Part 228, Hours of Service of Railroad Employees
- Part 229, Railroad Locomotive Safety Standards
- Part 231, Railroad Safety Appliance Standards
- Part 232, Brake System Safety Standards
- Part 233, Signal Systems Reporting Requirements
- Part 235, Instructions Governing Applications for Approval of a Discontinuance
- Part 236, Rules, Standards and Instructions Governing the Installation, Inspection, Maintenance and Repair of Signal and Train Control Systems, Devices, and Appliances
- Part 237, Bridge Safety Standards
- Part 238, Passenger Equipment Safety Standards
- Part 239, Passenger Train Emergency Preparedness

- Part 240, Qualification and Certification of Locomotive Engineers
- Part 242, Passenger Train System Safety Plans

The CHSTS will submit to the FRA any plans, programs, and procedures that affect the safe operation of the system, or which are required to demonstrate compliance with the applicable regulations.

Throughout Preliminary Engineering and Final Design phases the CHSTS will communicate with FRA to assure knowledge of the system as it is developed. CHSTS will maintain regular contact with FRA during development of operating rules, training of maintenance and operating personnel and development of operating practices prior to the start of revenue service.

As detailed in Section 7.0 of this SSMP the CHSTS will manage a safety and security certification program to record and demonstrate that all safety and security requirements for the project are identified and integrated into the final system.

10.2 Implementation

The CHSTS, through the Program Management Team, will maintain communications with the FRA representatives throughout the Planning, Preliminary Engineering, Final Design, Construction, and Testing and Start-up phases.

10.3 Coordination Process

Interface and coordination with FRA will be conducted through the PMT. The PMT will designate those persons authorized to interface with agents of the FRA to assure that information and decisions communicated between CHSTS and FRA are consistent, correct and authorized.

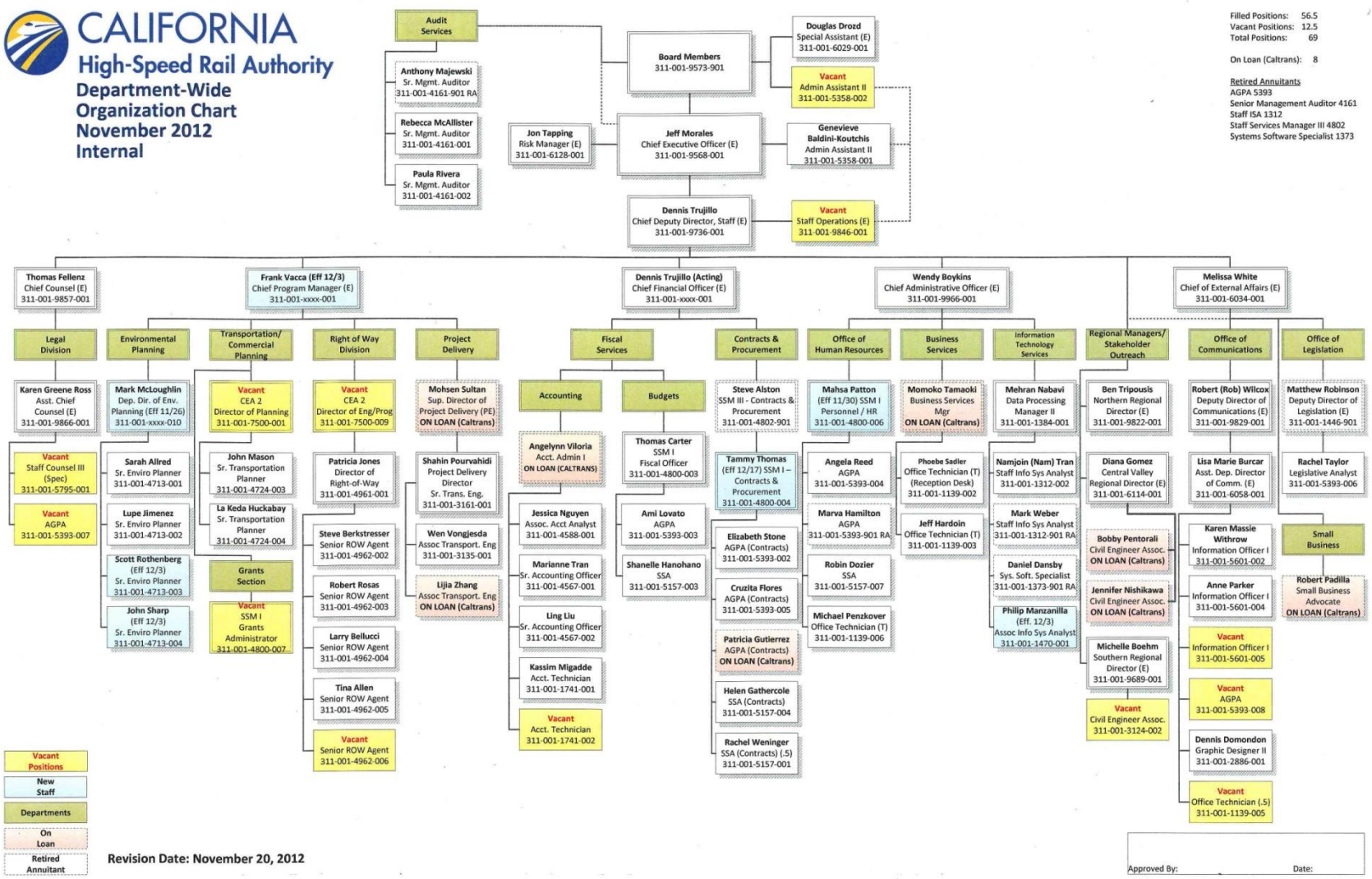
The FRA will provide guidance to the PMT with regard to applicable regulations, documents that will require formal submission and approval, and how any variances may be processed.

11.0 DEPARTMENT OF HOMELAND SECURITY COORDINATION

There are currently no DHS requirements or security directives that have been issued by the Transportation Security Administration (TSA) applicable to new builds, and particularly high-speed rail. The Authority will develop a Security and Emergency Preparedness Plan (SEPP) prior to revenue operation. The SEPP will fulfill DHS/TSA requirements for an operating railroad, which include development of an SEPP, and designating a primary and alternate Security Coordinator and providing TSA with names and contact information for 24 hour/7 days per week availability. The Security Coordinator will have a direct reporting relationship to the Authority Chief Executive Officer regarding matters of security.

The Authority has established liaison with the TSA Mass Transit and Rail Department through the project's lead security consultant who reports directly to the project operations manager. This liaison has been established to ensure all DHS/TSA requirements will be met once the project is complete, and to stay current with all security concerns, threats, best practices and developing security regulations that affect rail security.

APPENDIX A – CALIFORNIA HIGH-SPEED RAIL AUTHORITY ORGANIZATIONAL CHART



APPENDIX B – CHSTS CONSTRUCTION SAFETY PROGRAM REQUIREMENTS

1. CHSTS Construction Safety and Security Program

1.1 Program Goals and Objectives

The Construction Safety Program is established by the California High-Speed Rail Authority (Authority) to implement safety initiatives associated with the construction of the California High Speed Train System (CHSTS) and all other construction, repair, maintenance, and related services required by the Authority. The Construction Safety Program applies to all persons or entities involved in the warranty service of the post-construction California High-Speed Train System, including but not limited to the Authority and Program Management Team personnel, and warranty service Contractors (prime contractors and subcontractors).

Construction Safety and Security Program goals are as follows:

- Prevent personal injuries and property damage or loss
- Provide safe and secure work environment for employees, contractors, passengers, emergency responders, and the public at large
- To convey the CHSTS Safety and Security Policy Statement to all warranty service Contractors and sub-contractors
- To ensure compliance with the stated objectives and requirements contained in the CHSTS Safety and Security Policy Statement; Contractor's Site-Specific Health and Safety Plan (SSHASP); contract provisions; applicable federal, state and local laws and regulations; and industry consensus standards
- To identify specific requirements for the Warranty service Contractors' workplace safety and security programs
- To identify a process for Authority approval of the SSHASP and SSSP submittals.

The effectiveness of the Construction Safety Program depends upon active participation, cooperation, and compliance by Authority staff, Authority's Program Management Team (PMT) staff, and Contractors (and sub-contractors) project managers, superintendents, supervisors, and employees. Direct coordination with and between all parties is essential to the successful application of the following objectives:

- Plan and execute all Work to prevent personal injury, property damage or loss
- Comply with federal, state, and local laws, ordinances, regulations, industry consensus standards; and Authority and contractor regulations, policies, procedures, and requirements
- Implement and maintain a system of prompt identification and correction/abatement of unsafe and unhealthy practices and conditions
- Implementation and maintain a system of prompt detection and reporting of security breaches, incidents of conditions.
- Prompt notification and investigation of all incidents of injury, damage, or near-miss incidents to determine causes and take necessary corrective action
- Establish and conduct an educational program to stimulate and maintain the interest and cooperation of all employees through safety and security meetings and training programs

- Proper utilization of Personal Protective Equipment and all required safety equipment/devices
- Employ capable/competent personnel and develop processes providing safe and secure working environments for the construction work force, management facilities, the affected public, and private businesses and their properties
- Establish and maintain a comprehensive security program encompassing personnel, facility, and site management in conjunction with emergency planning and response procedures

1.2 California High-Speed Rail Authority Responsibilities

The California High-Speed Rail Authority is responsible for ensuring that the CHSTS is designed, built, tested, and placed into revenue service in a safe and secure manner. To that end, the Authority is responsible for the following:

- Formulation and implementation of acceptable policies, processes, work practices, and standards to promote the goals of the safety and security program
- Compliance with existing federal, state, and municipal statutory and regulatory safety and health laws, standards, codes, regulations, etc.

The Authority shall provide oversight and guidance with respect to the application and enforcement of the CHSTS Safety and Security Policy Statement (Section 1.25.1 of this contract section). The Authority shall audit the Contractor's activities and documentation to ensure compliance with the CHSTS Safety and Security Policy Statement and the approved Site-Specific Health and Safety Plan. The Authority may choose to delegate oversight responsibility for safety and security to a Program Management Team. Reference to the "Authority" in this contract section includes the Authority's Program Management Team or other designated representative.

1.3 Contractor Responsibilities

The Contractor is responsible for ensuring safety and security at all of its work sites, including the activities of subcontractors. Safety and security management and enforcement for each contract shall be administered by employees (direct hire) of the Contractor. This responsibility shall not be delegated nor contracted out to subcontractors, suppliers, consultant service/company, or any other persons/agency without written approval from the Authority. In compliance with these provisions, the Contractor shall perform the following:

- Perform a Job Hazard Analysis (JHA) for each job assignment within the scope of the contract for which a person may be exposed to incidents of injury or illness. JHAs previously performed by the Contractor will be acceptable for use in determining preventative measures if the scope and functionality of the jobs under review are justifiably the same. The previously-performed JHAs, however, must address the specific characteristics of each site and tasks performed within the project scope. JHAs shall be documented in electronic format and available for review by the Authority at any time.

- Develop a Site-Specific Health and Safety Plan (SSHASP) which shall address field work-related hazards and mitigation measures. The SSHASP must:

  - Consider all work to be performed by the Contractor (including any activities subcontracted);
  - Conform to the Contractor's corporate work site health and safety program;
  - Conform to applicable workplace safety regulations including but not limited to California Code of Regulations Title 8 Construction Safety Orders, Federal Railroad Administration regulations as found at 49CFR214, 49CFR219, 49CFR225, 49CFR228, 49CFR236, CPUC General Orders, Federal and State OSHA regulations; and,
  - Meet the SSHASP element requirements identified in Section 1.4 of this appendix.

- Develop a Site-Specific Security Plan (SSSP) which shall address field work-related threats/vulnerabilities and mitigation measures. This plan must:
  - Consider all work to be performed by the Contractor (including any activities subcontracted);
  - Conform to the Contractor's corporate work site security program; and,
  - Meet the element requirements identified in Section 1.5 of this appendix.
- Plan and execute all work in compliance with the stated objectives and requirements contained in the *CHSTS Safety and Security Policy Statement*; Contractor's SSHASP and SSSP; contract provisions; applicable federal, state and local laws, regulations; and industry consensus standards
- Ensure all subcontractors, suppliers, etc. are provided with a copy of the *CHSTS Safety and Security Policy Statement*, and Contractor's SSHASP and SSSP, and are properly informed of their obligations with regards to compliance.
- Participate in and support applicable safety and security certification processes as identified in Section 7.0 of the SSMP.
- Designate one or more persons as the safety and security representatives responsible to ensure the proper implementation of the SSHASP and SSSP respectively. Identify the response plan for the representative(s) and reporting responsibilities. The representatives will have sufficient knowledge and experience to demonstrate competency for applicable subject matter. The minimum qualifications shall be five years of diversified construction health and safety experience, 30 hour OSHA outreach Construction Training card, competent person training certifications for trenching and excavations, confined space entry and rescue (as applicable), tunnel construction and ventilation (as applicable), fall protection, certification as a Construction Health and Safety Technician (CHST), Certified Safety Professional (CSP), or Certified Industrial Hygienist (CIH), and two years experience related to the Contract scope of work. The qualifications of proposed safety and security representatives shall be submitted to the Authority for review and approval 30 days prior to field work taking place.
- The contractor shall be responsible for obtaining permits from the California Division of Occupational Safety for the following:
  - Construction of trenches or excavations which are five feet or deeper and into which a person is required to descend
  - Erection or demolition of any building, false work, scaffolding, or structure the equivalent 36 feet or higher
  - Performing any work related to hazardous materials
  - Performing any work subject to Cal/OSHA Tunnel Safety Orders

  Permits will be kept on file at the work site and available for immediate review upon request by the Authority.
- For any engineering or construction equipment (such as drills, cranes, concrete pump trucks, back hoes, and the like) that could encroach into the operating right-of-way of other railroads, the Contractor shall comply with the requirements of the other railroads including obtaining permits and taking the necessary precautions to be taken to preclude any accidental encroachment of the right-of-way. Encroachment shall be as defined by the other railroads and may include equipment such as cranes which could swing into or fall into the right-of-way. The Contractor will comply with the safety requirements specified by the adjacent railroad for work in and adjacent to other railroad's rights-of-way.

- For any engineering or construction equipment (such as drills, cranes, concrete pump trucks, back hoes, and the like) that could encroach into public right-of-way, such as streets and highways, the Contractor shall submit and obtain Authority Representative's approval and approval from local authorities having jurisdiction over the public right-of-way of a plan describing the use of such equipment and the precautions to be taken to preclude any accidental encroachment to the public right-of-way. Encroachment shall be understood to include equipment such as cranes which could swing into or fall into the public operating right-of-way. The Contractor shall comply with the safety requirements of the local authorities having jurisdiction over the operating right-of-way for work in and adjacent to that right-of-way.

1.4 Site-Specific Health and Safety Plan Elements

The safety processes, equipment utilized, and personnel assignments to be provided by the Contractor at each work site may differ based upon a site-specific Job Hazard Analysis (JHA) performed by the Contractor. The Site-Specific Health and Safety Plan shall include, but not be limited to, the following elements:

- Safety and security policy statement
- Identification of the makeup, reporting structure, and inter-action processes of the Contractor's Site Warranty Service Team, including the Contractor's Safety Manager, with the rest of the project work force (including sub-contractors and the Authority), and with third-parties such as emergency responders, utilities, and adjacent railroad operators
- Identification of roles and responsibilities of all employees for the Contractor and subcontractors with respect to safety
- Process for managing hazards or incident of injury or damage through identification, reporting, and correction or abatement or mitigation, including descriptions for processes and applicability of Job Hazard Analyses
- Procedures for work site safety audits and inspections, including assignment of responsibility, frequency, documentation method, and actions following various audit results
- Employee communication program that identifies individual responsibilities for all employees, schedules for specific communication techniques, and a process for recording and tracking communication program performance. The employee communication program will include but not be limited to:
    - Job briefing procedures/requirements
    - Hazard communications (HazComm)
    - Employee safety committees
    - Project safety committees
    - Notification to employees and the Authority of incidents or hazards when identified
- Site-specific workplace health and safety rules and procedures that conform to regulatory requirements of local, state, and federal occupational safety and health regulations, including but not limited to California Code of Regulations Title 8 Construction Safety Orders, Federal Railroad Administration regulations 49 CFR 200-299, California MUTCD, the Contractor's corporate safety plan, and the CHSTS Safety and Security Policy Statement. Rules and procedures must address site-specific work activities and conditions including but not limited to the following:
    - Personal protective equipment for all work site hazards and conditions, including equipment issuance/availability procedures

- Mobile equipment operation procedures and training program, including qualification process and requirements, and performance observation/evaluation requirements
- Fall protection and scaffolding procedures, including minimum fall protection equipment requirements, a process for training workers, and performance observation/evaluation requirements
- Motor vehicle operation program, including rules and procedures for specific equipment to be used at the work site (including industrial lift trucks), operator screening and qualification process and requirements, and performance observation/evaluation requirements
- Roadway worker protection (on-track safety) for Authority right-of-way in compliance with FRA regulations contained in 49 CFR Part 214
- Hazardous materials handling and storage plan specific to each work site, including a plan for cataloguing Material Safety Data Sheets and submitting same to the Authority, and for communicating MSDS information to employees
- Lockout/tagout programs for all applicable energy sources, including but not limited to electrical, hydraulic, and kinetic
- Fire prevention and suppression plan, including procedures for identification of hazards that could lead to fire, procedures for local fire suppression and notification to authorities, inspection processes, and a detailed training and exercise program
- Safety and security program training requirements and documentation including training curriculum, frequencies of and method of delivery for training, training records and lists of qualified/competent persons for specific tasks
- Roadway worker protection for adjacent railroad right-of-ways. Employees working in these locations shall be trained by the Contractors to ensure they become fully familiar with railway operations, procedures, rules, and safety requirements; and a daily Jobsite Hazard Analysis (JHA) shall be conducted.

- A plan for coordinating roadway worker protection activities and compliance with adjacent railroads. All Contractors working in the shared corridor will meet frequently with the responsible representatives of the operating railway and coordinate activities to minimize risks and hazards to Contractor personnel, and to avoid hazards or disruptions to the operation of the railway.
- Work site first-aid resources and a training program for employees
- An Emergency Response Plan for management of emergency situations associated with, but not limited to, the following: injury to an employee or member of the public; fire; flood; earthquake; property damage and damage to various utilities (such as, electrical, gas, sewage, water, telephone or public roadways); public demonstrations; acts of sabotage including threats of sabotage; hazardous materials encountered; toxic spills; explosions; vehicular accidents; and confined space rescues. The Emergency Response Plan shall be updated when conditions or procedures change. The Emergency Response Plan shall include the following: items, at minimum:
  - Identification of the person responsible for handling an emergency
  - Establishment of teams for handling each type of emergency
  - Identification of the person responsible for making emergency call (preferably the ranking Supervisor present)
  - The requirement to conspicuously post a list of an emergency phone numbers, along with information to be transmitted. Include with the emergency phone numbers, the number of the Authority representative to be contacted. Request telephone number and name of Authority contact person or persons from the Authority Representative.

  - Trench and confined space rescue plan or tunnel evacuation plan, as applicable
  - The procedure for contacting the Authority Representative when an incident of emergency response occurs
  - Scene management for the emergency response including procedures for ensuring the safety of employees and emergency responders, safeguarding the scene from unwanted entry, and handling on-scene media
- A plan for ensuring public safety at work sites and avoiding damage to public property. The public shall be considered as any persons and property not employed or owned by the Contractor or its Subcontractors. The plan must address site-specific work activities and conditions including but not limited to the following:
  - Identification of potential hazards to the public
  - Erection and proper warranty service at all times of all necessary safeguards for the protection of the public, including pedestrian and vehicle traffic, and the assignment of trained and competent flaggers whose sole duties shall consist of directing the movement of public traffic through or around the Work site
  - Posting of signs warning against the hazards created by warranty service activities
  - Elimination of unnecessary noise, obstructions, and other annoyances to nearby residents and businesses
  - Procedures and competency training for employees assigned to public safety and public property protection
  - Designated work zones. Work outside of the designated work zones shall be performed only when specifically stated in writing from the Authority Representative.
- Other elements that conform to the Contractor's corporate health and safety plan.

1.5 Site-Specific Security Plan Elements

Security at construction sites is to ensure all personnel working at the site, and the surrounding communities, are protected from crime and security-related conditions. This includes protection of materials, tools, equipment and personal property of workers at sites. Each construction site will vary, from type of equipment, machinery, materials and tools to adjacent public and private areas and local zoning ordinances. The types of security to be provided by the Contractor at each construction site may differ based upon a site-specific security assessment performed by the Contractor. The Site-Specific Security Plan shall include, but not be limited to, the following elements:

- Safety and security policy statement
- Identification of the makeup, reporting structure, and inter-action processes of the Contractor's Project Management Team, including the Contractor's Security Management Team, with the rest of the project work force (including sub-contractors and the Authority) and with third-parties such as local law enforcement agencies
- Identification of roles and responsibilities of all employees for the Contractor and subcontractors with respect to security
- Protection of the public and property, materials, equipment and tools through the use of fencing, access control, locks, alarms, intrusion detection, lighting, and security guards as necessary, and any other security requirements that may be applicable

- Personnel security program including employee background requirements, a code of conduct and expectations for employee behavior, and procedures for internal and external notification when personnel security is violated
- Access control program to identify authorized persons for each work site, procedures for authorizing new employees or visitors, and procedures for monitoring access control performance
- Plan for coordination with local law enforcement for incident reporting, traffic control and other security related conditions or events
- Other elements that conform to the Contractor's corporate security plan